DER GRÖSSTE GEMEINSCHAFTLICHE TEILER VON ALGEBRAISCHEN ZAHLEN ZWEITER ORDNUNG MIT NEGATIVER DISKRIMINANTE UND DIE ZERLEGUNG DIESER ZAHLEN IN PRIMFAKTOREN

INAUGURAL-DISSERTATION

DER HOHEN MATHEMATISCHEN UND
NATURWISSENSCHAFTLICHEN FAKULTÄT
DER KAISER-WILHELMS-UNIVERSITÄT ZU STRASSBURG
ZUR ERLANGUNG DER DOKTORWÜRDE

VORGELEGT VON

JAKOB SCHATUNOVSKY
AUS WOSNESENSK (SÜD-RUSSLAND)

DRUCK VON B. G. TEUBNER IN LEIPZIG 1912

DER GRÖSSTE GEMEINSCHAFTLICHE TEILER VON ALGEBRAISCHEN ZAHLEN ZWEITER ORDNUNG MIT NEGATIVER DISKRIMINANTE

UND DIE ZERLEGUNG DIESER ZAHLEN IN PRIMFAKTOREN

INAUGURAL-DISSERTATION

DER HOHEN MATHEMATISCHEN UND
NATURWISSENSCHAFTLICHEN FAKULTÄT
DER KAISER-WILHELMS-UNIVERSITÄT ZU STRASSBURG
ZUR ERLANGUNG DER DOKTORWÜRDE

VORGELEGT VON

JAKOB SCHATUNOVSKY
AUS WOSNESENSK (SÜD-RUSSLAND)

DRUCK VON B. G. TEUBNER IN LEIPZIG 1912

Gedruckt mit Genehmigung
der mathematischen und naturwissenschaftlichen Fakultät Straßburg.
Referent: Prof. Dr. H. Weber.

Vorwort.

Die vorliegende Schrift ist eine Untersuchung über die Erweiterung des größten gemeinschaftlichen Teilers, sowie des Euklidischen Algorithmus für diejenigen ganzen algebraischen Zahlen, für welche die Zerlegung in unzerlegbare Faktoren eindeutig ist. Ferner ist der Aufbau eines Algorithmus bezweckt, welcher dasselbe Ziel verfolgt für die Fälle, wo der Euklidische Algorithmus versagt.

In dem großen Werke von R. Dedekind „Vorlesungen über Zahlentheorie von Lejeune Dirichlet“ vierte Auflage § 159 ist diese Aufgabe für den Gaußschen Körper erledigt. Diese Untersuchung schließt mit folgenden Worten:

„Genau in derselben Weise, wie hier die ganzen komplexen Zahlen $x + yi$ untersucht sind, werden sich noch manche andere Gebiete von ganzen Zahlen behandeln lassen“.

Diese Äußerung gab den Anlaß zur vorliegenden Arbeit. Da es nun Fälle gibt, wo die Zerlegung in unzerlegbare Faktoren eindeutig ist, der Euklidische Algorithmus aber nicht anwendbar, so hat sich diese Aufgabe geändert, und wir haben diese Aufgabe für alle solche Körper mittels des Matrizenkalkul zu lösen versucht. Es hat sich aber herausgestellt, daß die Aufgabe sich auf Rechnungen mit ganzen rationalen Zahlen zurückführen läßt und dadurch ist diese Arbeit ganz elementar geworden.

Die im folgenden benutzten Werke sind:

R. Dedekind „Vorlesungen über Zahlentheorie von Lejeune Dirichlet“

H. Weber „Algebra“

C. Gauß „Disquisitiones arithmeticae“

P. Tschebyscheff „Theorie der Kongruenzen“

I. Sommer „Vorlesungen über Zahlentheorie“

Die Lösung der gestellten Aufgabe ist in §§ 3—5 enthalten. In den § 6 und 7 folgen wir den angegebenen Werken. In diesen Paragraphen soll gezeigt werden, wie die bei Anwendung der gegebenen Lösung entstehenden Schwierigkeiten möglichst beseitigt werden können.

Es sei mir noch gestattet, meinem hochverehrten Lehrer, Herrn Prof. Dr. H. Weber, der mich auf das Thema aufmerksam machte und mir wertvolle Anregungen gab, meinen herzlichsten Dank auszusprechen.

Einteilung.

§ 1. Die quadratischen imaginären Zahlen 1
§ 2. Die Normen der quadratischen imaginären Zahlen und der Begriff „Größter gemeinschaftlicher Teiler“ dieser Zahlen 6
§ 3. Der Euklidische Algorithmus für eindeutig zerlegbare quadratische Zahlen mit negativer Diskriminante 9
§ 4. Die Bestimmung des größten gem. Teilers für eindeutig zerlegbare quadratische imaginäre Zahlen mittels der Normen dieser Zahlen 28
§ 5. Die Zerlegung von eindeutig zerlegbaren quadratischen imaginären Zahlen in unzerlegbare Faktoren. 36
§ 6. Behandlung der Gleichung
$$x^2 + Dy^2 = k$$
für große k 42
§ 7. Die Faktorenzerlegung der quadratischen Form
$$a^2 + Db^2.$$ 51
Kurze Zusammenstellung des Inhaltes 59

§ 1. Die quadratischen imaginären Zahlen.

Bezeichnet ν die Gesamtanzahl der reellen, sowie der Paare von imaginären Permutationen des Körpers Ω, so gibt es in o, wo o der Inbegriff aller in Ω enthaltenen ganzen algebraischen Zahlen ist, immer $\nu-1$ Fundamentaleinheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ von solcher Beschaffenheit, daß, wenn man dieselben beliebig oft miteinander multipliziert und dividiert und dem so gebildeten allgemeinen Produkt die sämtlichen in o enthaltenen Einheitswurzeln δ, deren Anzahl φ stets endlich ist, einzeln als Faktor zusetzt, so werden alle Einheiten in o und zwar jede nur einmal dargestellt.[1])

Es sind also in der Form $\varepsilon = \delta \varepsilon_1^{l_1} \varepsilon_2^{l_2} \ldots \varepsilon_{\nu-1}^{l_{\nu-1}}$ alle Einheiten des Körpers jede nur einmal enthalten, wenn $l_1, l_2, \ldots, l_{\nu-1}$ beliebige Kombinationen von ganzen rationalen Zahlen sind; z. B. in dem Zahlenkörper $R(\sqrt{10})$ gehen die Zahlen $3+\sqrt{10}$, $3-\sqrt{10}$, $19+6\sqrt{10}$, $19-6\sqrt{10}$, $117+37\sqrt{10}$, $117-37\sqrt{10}$, usw. in 1 auf, was aus der Gleichung

$$(-1)^n = (3+\sqrt{10})^n \cdot (3-\sqrt{10})^n$$

folgt.

Der einfachste Fall, nämlich $\nu = 1$, tritt bei den imaginären quadratischen Körpern ein. Für diese Körper läßt sich in folgender einfacher Weise neben deren einfachstem Ausdruck auch die Anzahl der Einheiten genau angeben.

Satz 1: *Die ganzen Zahlen eines quadratischen imaginären Körpers sind in der Form*

$$\frac{a \pm b\varrho}{2}$$

enthalten. Dabei sind die Zahlen a und b ganze rationale Zahlen, $\varrho = \sqrt{-D}$, *die Zahl D ist rational, positiv und enthält keine quadratischen Faktoren.*

Beweis: Die Gleichung

$$x^2 + px + q = 0$$

hat die Wurzeln

$$x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

---

1) R. Dedekind „Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet", vierte Auflage, § 183 p. 602.

Setzen wir $-p = a$, und $p^2 - 4q = -b^2 D$, worin D keine quadratischen Faktoren enthält, so ist

$$\frac{-p \pm \sqrt{p^2 - 4q}}{2} = \frac{a \pm b\sqrt{-D}}{2} = \frac{a \pm b\varrho}{2},$$

q. e. d.

Dieser Satz läßt sich nur teilweise umkehren, nämlich

Satz 2: *Die Zahlen* $\frac{a \pm b\varrho}{2}$ *für die eben angegebenen* a, b *und* ϱ *sind nur dann ganz, wenn zugleich* $\frac{a^2 + Db^2}{4}$ *ganz ist.*

Beweis: Setzen wir

$$x_1 = \frac{a + b\varrho}{2},\ x_2 = \frac{a - b\varrho}{2},\ \text{so ist}\ x_1 + x_2 = a,\ x_1 x_2 = \frac{a^2 + Db^2}{4},$$

so sind x_1 und x_2 Wurzeln einer und derselben Gleichung

$$x^2 - ax + \frac{a^2 + Db^2}{4} = 0.$$

Soll demnach x_1 ganz sein, so muß $\frac{a^2 + Db^2}{4}$ eine ganze rationale Zahl sein, damit man durch diese Gleichung eine ganze algebraische Zahl α_1 definieren kann.

Aus diesem Satz folgt unmittelbar der folgende

Satz 3: *Ist* $\frac{a \pm b\varrho}{2}$ *für die angegebenen* a, b *und* ϱ *eine ganze Zahl, so sind* a *und* b *beide zugleich gerade oder ungerade.*

Beweis: Daraus, daß in diesem Fall $\frac{a^2 + Db^2}{4}$ eine ganze Zahl ist, folgt, daß, wenn a gerade ist, Db^2 durch 4 teilbar sein muß, weil aber D keine quadratischen Faktoren enthält, so ist b^2 also auch b eine gerade Zahl. Wenn a ungerade ist, so ist auch a^2 und infolgedessen auch Db^2, also auch b ungerade.

Damit Db^2 ungerade sein kann, muß übrigens D ungerade sein. Ist also D eine gerade Zahl, so können a und b nur gerade Zahlen sein. Ist aber $a = 2a_1$, $b = 2b_1$, so ist $\frac{a + b\varrho}{2} = a_1 + b_1\varrho$ und das muß für D-geraden immer der Fall sein.

Satz 4: *Die Zahlen* $\frac{a + b\varrho}{2}$, *wo* a *und* b *beide ungerade sind, sind nur, wenn* $\frac{1 + D}{4}$ *eine ganze rationale Zahl ist, ganz.*

Beweis: Ist $a = 2a_1 + 1$, $b = 2b_1 + 1$, so ist

$$\frac{a^2 + Db^2}{4} = \frac{4a_1^2 + 4a_1 + 1 + 4Db_1^2 + 4Db_1 + D}{4}$$

also muß $\frac{1 + D}{4}$ eine ganze Zahl sein, wenn nicht, so kann $\frac{a + b\varrho}{2}$ nicht ganz sein.

Ist $\frac{a^2+Db^2}{4}=1$, so sind die Zahlen $\frac{a+b\varrho}{2}$ und $\frac{a-b\varrho}{2}$ als Teiler der Zahl 1 Einheiten und umgekehrt — sind das Einheiten, so ist ihr Produkt $\frac{a^2+Db^2}{4}$ ein Teiler der Zahl 1, also als ganze rationale Zahl gleich 1.

Ist aber $\frac{a^2+Db^2}{4}=1$, so ist $a^2+Db^2=4$, und jedes Lösungspaar der Gleichung $x^2+Dy^2=4$ bietet uns demnach eine Einheit im betrachteten Körper. Diese Gleichung hat aber, wenn $D>4$ ist oder $=2$ ist, nur die zwei Lösungen $x=\pm 2$, $y=0$, und es gibt also in diesem Körper, wie im Körper der rationalen Zahlen, nur die zwei Einheiten ± 1, es bleiben noch besonders die Fälle $D=1$ und $D=3$. Ist $D=1$, so findet man vier Einheiten ± 1, $\pm i$, ist $D=3$, so sind ± 1, $\pm\frac{-1+\sqrt{-3}}{2}$, $\pm\frac{-1-\sqrt{-3}}{2}$ die sechs Einheiten dieses Körpers. Damit ist zugleich der folgende Satz bewiesen.

Satz 5: *In dem Körper $R(\sqrt{-3})$ gibt es sechs Einheiten, das sind ± 1, $\pm\frac{-1+\sqrt{-3}}{2}$, $\pm\frac{-1-\sqrt{-3}}{2}$, in dem Gaußschen gibt es vier, das sind ± 1, $\pm i$, in allen anderen quadratischen imaginären Körpern gibt es nur die zwei Einheiten ± 1.*

Wir werden zwei algebraische Zahlen, welche sich durch eine Einheit unterscheiden, als nicht wesentlich verschieden betrachten, weil jede Zahl durch 1 und also durch jede Einheit teilbar ist. Solche Zahlen heißen auch „assoziierte“.

Die Sätze der Teilbarkeit, welche für ganze rationale Zahlen gelten, sind für die algebraischen nicht alle gültig. Es ist nämlich die Eindeutigkeit der Zerlegung in unzerlegbare Faktoren nicht immer erfüllt. Um das zu beweisen, brauchen wir nur ein einziges Beispiel dafür anzuführen. Betrachten wir die Zahl 21 in dem Körper $R(\sqrt{-5})$, so ist

$$21=3\cdot 7=(4+\sqrt{-5})(4-\sqrt{-5})=(1+2\sqrt{-5})(1-2\sqrt{-5}).$$

Die Mehrdeutigkeit dieser Zerlegung folgt aus dem Beweis, daß die Zahlen 3, 7, $4+\sqrt{-5}$, ... unzerlegbar sind.

Die ganzen Zahlen $\frac{a+b\varrho}{2}$ kommen in dem Körper $R(\sqrt{-5})$ nicht in Betracht (Satz 4). Nehmen wir an, daß 7 in zwei Faktoren, von welchen keiner eine Einheit ist, zerlegbar ist, dann ist

$$7=(x+y\sqrt{-5})(x_1+y_1\sqrt{-5})=(xx_1-5yy_1)+(xy_1+yx_1)\sqrt{-5}$$

also

$$xx_1-5yy_1=7,\quad xy_1+yx_1=0\quad\text{oder}\quad x=-\frac{yx_1}{y_1}.$$

Die Zahlen x und y auch x_1 und y_1 müssen wir im rationalen Körper ganz und relativprim voraussetzen, also muß $\frac{y}{y_1} = Q$ ganz sein, weil x ganz ist, also ist $x = -x_1 Q$ und $y = y_1 Q$. Setzen wir diese Werte in die erste Gleichung ein, so folgt

$$-x_1^2 Q - 5y_1^2 Q = 7 \text{ oder } -Q(x_1^2 + 5y_1^2) = 7.$$

Da aber hier lauter ganze rationale Zahlen vorkommen, $x_1 + y_1\sqrt{-5}$ keine Einheit und $x_1^2 + 5y_1^2$ eine ganze positive von 1 verschiedene Zahl ist, so ist

$$-Q = 1,\ x_1^2 + 5y_1^2 = 7.$$

Dies ist jedoch unmöglich; denn würde $x_1^2 + 5y_1^2 = 7$ für ganze rationale Zahlen gelten, so würde $x_1^2 = 7 - 5y_1^2$ sein. Für $y_1 = 0$ und ± 1 kann aber x_1 nicht rational sein, ferner wird für alle anderen rationalen ganzzahligen y_1 die Zahl x_1^2 negativ und dies ist unmöglich.

In derselben Weise läßt sich auch die Zahl 3 behandeln.

Die Zahl $4 + \sqrt{-5}$ werden wir in folgender Weise untersuchen. Nehmen wir an, daß

$$4 + \sqrt{-5} = (x + y\sqrt{-5})(x_1 + y_1\sqrt{-5}) = (xx_1 - 5yy_1) + (xy_1 + yx_1)\sqrt{-5};$$

also ist

$$4 - \sqrt{-5} = (xx_1 - 5yy_1) - (xy_1 + yx_1)\sqrt{-5} = (x - y\sqrt{-5})(x_1 - y_1\sqrt{-5})$$

und wir bekommen durch Multiplikation

$$21 = (x^2 + Dy^2)(x_1^2 + Dy_1^2).$$

Es muß also entweder

$$x^2 + 5y^2 = 3$$

oder

$$x^2 + 5y^2 = 7$$

sein. Das ist aber, wie bewiesen, unmöglich. Damit ist zugleich bewiesen, daß auch $4 - \sqrt{-5}$ unzerlegbar ist, und ebenso lassen sich auch die übrigen Faktoren von 21 behandeln.

Dieses Beispiel zeigt, daß die eindeutige Zerlegung in Primfaktoren für algebraische Zahlen nicht immer statt hat. Die Begriffe und Sätze, welche für ganz rationale Zahlen gelten, lassen sich also auf die algebraischen nicht ohne weiteres übertragen, aber auch selbst, wenn die Gesetze der Teilbarkeit von ganzen rationalen Zahlen auch in bestimmten algebraischen Körpern richtig bleiben, so müssen wir doch ein Mittel suchen, die Gesamtheit von nicht wesentlich verschiedenen Zahlen zusammenfassen zu können. Diese beiden Aufgaben: die Mehrdeutigkeit der Zerlegung in Primfaktoren zu beseitigen und die nicht wesentlich verschiedenen Zahlen zusammenzufassen, lassen sich durch Einführung der sog. Ideale erledigen.

Der größte gemeinschaftliche Teiler von gegebenen algebraischen Zahlen läßt sich als Produkt von allen gemeinsamen Primidealen, also als ein Ideal darstellen. Als algebraische Zahl aufgefaßt, hat aber in diesem Falle der Begriff des größten gemeinschaftlichen Teilers keinen Sinn, so lange die algebraische Zahl nicht auch in Zahlen eindeutig zerlegbar ist. Wenn aber diese Zerlegung eindeutig ist, reduzieren sich die Ideale auf Zahlen dieses Körpers und ihre Einführung als Ideale ist überflüssig. Sie werden auch überflüssig zur Darstellung von allen nicht wesentlich verschiedenen Zahlen, wenn die Anzahl der Einheiten endlich ist. Die Eindeutigkeit der Zerlegung und Endlichkeit der Einheitsanzahl sind also die Bedingungen dafür, daß die Ideale als solche überflüssig sind, weil sie auf Zahlen des Körpers sich reduzieren. Diese Überlegungen veranlassen uns diejenigen Körper, welche die eindeutige Zerlegung in Primfaktoren zulassen und eine endliche Anzahl von Einheiten besitzen, auszusondern und für diese Körper ein Mittel anzugeben den größten gemeinschaftlichen Teiler ohne Benutzung der Ideale zu finden.

Eine endliche Anzahl von Einheiten haben nur, wie gezeigt, die imaginären quadratischen Körper. Wir brauchen also nur diese in Betracht zu ziehen.

Unter denselben sind aller Wahrscheinlichkeit nach nur die mit den Diskriminanten

$$-1, -2, -3, -7, -11, -19, -27, -43, -67, -163$$

und keine anderen eindeutig zerlegbar, weil aber die Werte von D für uns keine Rolle spielen, so werden wir hier nicht darauf eingehen. Ob es auch nicht quadratische Körper mit nur eindeutig zerlegbaren Zahlen gibt, ist für unsere Aufgabe wegen der unendlichen Einheitsanzahl auch nicht wesentlich. Übrigens sind unter den Körpern dritter und höherer Ordnung solche nicht gefunden. Ein allgemeines Kriterium zur Auffindung aller derartigen Körper oder ein Beweis dafür, daß solche nicht existieren, ist nicht bekannt.[1]) Die Lösung dieser Frage wäre zwar von großem Interesse, da wir aber alle diese Körper außer Betracht lassen, so werden wir hier auch auf sie nicht näher eingehen und wollen jetzt die Aufgabe ausführlich behandeln, den größten gemeinschaftlichen Teiler für imaginäre quadratische eindeutig zerlegbare Zahlen zu finden.

1) H. Weber „Algebra“ Bd. III, p. 460.

§ 2. Die Normen der quadratischen imaginären Zahlen und der Begriff „größter gemeinschaftlicher Teiler" dieser Zahlen.

Die Sätze der Teilbarkeit, welche wir brauchen, lassen sich auf die zu untersuchenden Zahlen durch Einführung von Normen übertragen. Nehmen wir unsere Zahl in der Form

$$m + n\varrho, \quad \varrho = \sqrt{-D}$$

an, wo m und n ganze Zahlen oder die Hälfte von solchen sind, so nennt man $m - n\varrho$ die zu $m + n\varrho$ konjugierte Zahl und das Produkt

$$(m + n\varrho)(m - n\varrho) = m^2 + Dn^2$$

die Norm derselben. Aus der Bildung der Norm folgt, daß der Zahl $m + n\varrho$ die Norm $m^2 + Dn^2$ eindeutig zugeordnet ist. Über die Norm einer Zahl ergeben sich von selbst folgende Sätze.

Satz 1: *Die Norm eines Produktes ist gleich dem Produkt der Normen der einzelnen Faktoren,* denn, wenn

$$m + n\varrho = (m_1 + n_1\varrho)(m_2 + n_2\varrho) \cdots (m_t + n_t\varrho) \text{ ist,}$$

so ist auch

$$m - n\varrho = (m_1 - n_1\varrho)(m_2 - n_2\varrho) \cdots (m_t - n_t\varrho)$$

also infolge der Multiplikation

$$N(m + n\varrho) = N(m_1 + n_1\varrho)\, N(m_2 + n_2\varrho) \cdots N(m_t + n_t\varrho).$$

Satz 2: *Die Norm eines Quotienten ist gleich dem Quotient der Normen von Zähler und Nenner und umgekehrt.*

Beweis: $N\left(\frac{m + n\varrho}{r + s\varrho}\right) = \frac{m + n\varrho}{r + s\varrho} \cdot \frac{m - n\varrho}{r - s\varrho} = \frac{N(m+n\varrho)}{N(r + s\varrho)}$.

Eine Gleichung ist aber auch immer umkehrbar, daraus folgt die Umkehrung des Satzes.

Satz 3: $N(m + n\varrho)$ *ist eine ganze positive Zahl.*

Beweis: Ist $m = a$ und $n = b$, wo a und b ganze rationale Zahlen sind, so ist $N(m + n\varrho) = a^2 + Db^2$ — als Produkt und Summe von ganzen positiven rationalen Zahlen — ganz und positiv. Ist $m = \frac{a}{2}$ und $n = \frac{b}{2}$, so ist doch $N(m + n\varrho) = \frac{a^2 + Db^2}{4}$ ganz, weil $\frac{a + b\varrho}{2}$ eine ganze Zahl ist (Satz 2, § 1). Daß diese Zahl auch positiv ist, folgt daraus, daß a^2, D, b^2 positive Zahlen sind.

Satz 4: *Ist* $N(m + n\varrho) = 0$, *so muß* $m = 0$ *und* $n = 0$ *sein.*
Beweis:

$$N(m + n\varrho) = m^2 + Dn^2 = 0.$$

Weil D positiv ist, so ist das nur möglich, wenn $m^2 = 0$ und $Dn^2 = 0$ sind, folglich ist $m = 0$ und, weil D von 0 verschieden ist, so muß n^2 und infolgedessen $n = 0$ sein.

Für die zu untersuchenden algebraischen Zahlen müssen wir jetzt nur noch zwei Zahlen in Bezug auf die Normen nach der Größe vergleichen. Wir werden die Zahl $m + n\varrho$ normgrößer als $r + s\varrho$ nennen wenn $m^2 + Dn^2 > r^2 + Ds^2$, normkleiner, wenn $m^2 + Dn^2 < r^2 + Ds^2$ und normgleich, wenn $m^2 + Dn^2 = r^2 + Ds^2$ ist.

Die Begriffe „Normgrößer", „Normkleiner" und „Normgleich" müssen in jedem Begriff von „Größer", „Kleiner" und „Gleich" für algebraische Zahlen enthalten sein, sonst müssen wir zu einem Widerspruch kommen, wenn eine quadratische Zahl sich auf eine rationale reduziert.

Sind zwei Zahlen $m + n\varrho$ und $r + s\varrho$ normgleich, so können sie doch verschieden sein. Es ist z. B. $N(7 + 3\sqrt{-3}) = N(8 + 2\sqrt{-3}) = 76$. Aus allen normgleichen Zahlen werden wir nur diejenigen Zahlen $m + n\varrho$ und $r + s\varrho$ als gleich betrachten, bei welchen $m = r$ und $n = s$ ist.

Aus dieser Definition und aus dem Satz 4 folgt unmittelbar der folgende für uns wichtige Satz.

Satz 5: *Ist* $N(m + n\varrho) = 0$, *so ist* $m + n\varrho = 0$.

Diese Begriffe reichen aus um den Begriff „größter gemeinschaftlicher Teiler" für quadratische eindeutig zerlegbare imaginäre Zahlen einzuführen und seine Existenz und Eindeutigkeit zu beweisen.

Jedes Produkt $(m_1 + n_1\varrho)(m_2 + n_2\varrho) \cdots (m_t + n_t\varrho)$ ist wieder eine Zahl der Form $m + n\varrho$, also gibt es auch zusammengesetzte Zahlen. Haben zwei Zahlen $m + n\varrho$ und $r + s\varrho$ denselben Teiler $x + y\varrho$, so wird die Zahl $x + y\varrho$, als gemeinsamer Teiler von $m + n\varrho$ und $r + s\varrho$ betrachtet. Derjenige gemeinsame Teiler, welcher durch alle anderen gemeinsamen Teiler teilbar ist, wird als größter gemeinschaftlicher Teiler bezeichnet. Seine Eindeutigkeit wird dadurch bewiesen, daß jede der gegebenen Zahlen der Annahme nach aus eindeutig bestimmten unzerlegbaren Faktoren besteht. Dadurch werden alle gemeinsamen unzerlegbaren Faktoren und also ihr Produkt eindeutig bestimmt. Da aber jeder Teiler der gegebenen Zahlen aus eindeutig bestimmten unzerlegbaren Teilern besteht, so ist jeder gemeinsamer Teiler dieser Zahlen auch in diesem Produkt enthalten. Dieses Produkt können wir also als den größten gemeinschaftlichen Teiler der gegebenen Zahlen betrachten. Dadurch wird auch sein Existenzbeweis erbracht.

Ist $z + w\varrho$ der größte gemeinschaftliche Teiler für die Zahlen $m_1 + n_1\varrho$, $m_2 + n_2\varrho$, ..., $m_t + n_t\varrho$, so werden wir das symbolich in folgender Weise bezeichnen

$$z + w\varrho = g\,(m_1 + n_1\varrho,\ m_2 + n_2\varrho,\ \ldots,\ m_t + n_t\varrho).$$

Ist $z + w\varrho$ eine Einheit, so sind diese Zahlen teilerfremd. Die Begriffe „teilerfremd" und „relativprim" haben für algebraische Zahlen verschiedene Bedeutung. Das Relativprimsein ist von den Idealen abhängig, die wir nicht berücksichtigen.

Die Gleichung

$$A = BQ + R,$$

in welcher Q der Quotient und R der Rest von der Division A durch B ist, bleibt für die zu untersuchenden Zahlen nicht unbedingt erhalten in dem Sinne, daß $R < B$ ist, d. h. bilden wir die Gleichung

$$\frac{m + n\varrho}{r + s\varrho} = x + y\varrho + \frac{k + l\varrho}{r + s\varrho},$$

wo $x + y\varrho$ und $k + l\varrho$ ganze Zahlen sind, welche der Gleichung

$$m + n\varrho = (r + s\varrho)\,(x + y\varrho) + k + l\varrho$$

genügen und $N(k + l\varrho)$ möglich klein ist, so kann doch $N(k + l\varrho) > N(r + s\varrho)$ sein. Dies kann durch Angabe eines Beispiels bewiesen werden.

Wir dividieren $6 - \varrho$ durch $1 - \varrho$ und bekommen $1 - \varrho$ als Quotient und 5, als Rest, $\varrho = \sqrt{-19}$

$$6 - \varrho = (1 - \varrho) + 5$$

$N(-5) = 25$, $N(1 - \varrho) = 20$, also ist $N(-5) > N(1 - \varrho)$.

Da aber der Euklidische Algorithmus gerade auf der hier nicht unbedingt gültigen Ungleichung

$$R < B$$

beruht, so muß zuerst die Bildung der Fundamentalgleichung des Euklidischen Algorithmus

$$A = BQ + R$$

speziell untersucht werden.

§ 3. Der Euklidische Algorithmus für eindeutig zerlegbare quadratische Zahlen mit negativer Diskriminante.

Die ganzen quadratischen Zahlen $\frac{a+b\varrho}{2}$, wo a und b ganze rationale Zahlen sind, brauchen wir nur dann zu berücksichtigen, wenn $\frac{1+D}{4}$ ganz ist. Für andere D haben wir es nur mit Zahlen der Form $a+b\varrho$ zu tun. Aber auch bei $D=4t+3$ können wir uns von dem Nenner 2 befreien auf Grund des folgenden Satzes.

Satz 1: *Jede ganze quadratische Zahl $m+n\varrho$ läßt sich auf die Form $a+b\sigma$, wo a, b ganze rationale Zahlen und σ eine ganze Zahl desselben Körpers ist, bringen und umgekehrt.*

Beweis: Weil jede ganze Zahl σ sich auf die Form $\frac{x+y\varrho}{2}$ bringen läßt (Satz 1, § 1), so soll also

$$\frac{a+b\varrho}{2}=a_{\nu_1}+b_{\nu_1}\frac{x+y\varrho}{2}$$

sein oder

$$a+b\varrho=2a_{\nu_1}+b_{\nu_1}x+b_{\nu_1}y\varrho$$

also

$$b=b_{\nu_1}y,\quad a=2a_{\nu_1}+b_{\nu_1}x,$$

folglich

$$b_{\nu_1}=\frac{b}{y},\quad a_{\nu_1}=\frac{a-\frac{bx}{y}}{2}.$$

Die Zahlen a und b sind entweder beide gerade oder beide ungerade (Satz 3, § 1). Nehmen wir für y einen von 2 verschiedenen Teiler von b und für x eine beliebige ungerade Zahl, so sind a_{ν_1} und b_{ν_1} ganz.

Ist umgekehrt die Zahl $a_{\nu_1}+b_{\nu_1}\sigma$ ganz, so läßt sie sich auf die Form $\frac{a+b\varrho}{2}$ bringen.

$$a_{\nu_1}+b_{\nu_1}\sigma=a+\frac{bx}{2}+\frac{by\varrho}{2}=\frac{2a+bx}{2}+\frac{by}{2}\varrho.$$

Setzen wir darin $a=2a_{\nu_1}+b_{\nu_1}x$, $b=b_{\nu_1}y$, so ist diese Darstellung erreicht, a und b sind ganz, weil $b_{\nu_1}x$ und $b_{\nu_1}y$ ganz sind, weil aber $a_{\nu_1}+b_{\nu_1}\sigma$ ganz ist, so ist auch $\frac{a+b\varrho}{2}$ ganz.

Satz 2: *Ist auch σ_1 eine Zahl, welche zur Darstellung der Zahl $a+b\frac{\varrho}{2}$ in der Form $a_2+b_2\sigma_1$ sich eignet, so läßt sich $a_{\nu_1}+b_{\nu_1}\sigma$ in der Form $a_2+b_2\sigma_1$ darstellen.*

Beweis: $a_{\nu_1}+b_{\nu_1}\sigma = a_{\nu_1}+b_{\nu_1}\frac{x+y\varrho}{2} = \frac{a+b\delta}{2}$ (Satz 1)

also ist

$$a_{\nu_1}+\frac{b_{\nu_1}x}{2} = \frac{a}{2} \text{ und } b_{\nu_1}y = b.$$

Setzen wir

$$\frac{a+b\varrho}{2} = a_2+b_2\sigma_1 = a_2+b_2\frac{x_1+y_1\varrho}{2},$$

so ist

$$a = a_2+\frac{b_2x_1}{2},\quad b = b_2y_1,$$

weil σ_1 auch zur Darstellung der Zahl $\frac{a+b\varrho}{2}$ geeignet ist, so muß $b_2 = \frac{b}{y_1}$ eine ganze Zahl sein und ebenso ist $a_2 = a-\frac{bx_1}{y_1}$ auch ganz.[1])

Die Zahlen $a_1+b_1\sigma$ und $a_2-b_2\sigma_1$ werden wir jetzt als $a+b\sigma$ bezeichnen.

Wir werden auch die $N(a+b\sigma)$ bestimmen. Es sei

$$a+b\sigma = a+b\frac{x+y\varrho}{2} = \left(a+\frac{bx}{2}\right)+\frac{by\varrho}{2}$$

also ist die mit $a+b\sigma$ konjugierte Zahl

$$\left(a+\frac{bx}{2}\right)-\frac{by}{2}\varrho$$

und

$$(1)\quad N(a+b\varrho) = \left(a+\frac{bx}{2}\right)^2+\frac{Db^2y^2}{4} = a^2+b^2\frac{x^2+Dy^2}{4}+abx$$

Weil aber $a+b\sigma = m+n\varrho$ ist, so ist $a^2+b^2\frac{x^2+Dy^2}{4}+abx$ nur eine Umformung von $N(m+n\varrho)$, und es bleibt also alles, was wir für die Normen bewiesen haben, erhalten.

Auch für solche Körper, bei denen die ganzen Zahlen $\frac{a+b\varrho}{2}$ sich immer durch Kürzung auf die Form $a_1+b_1\varrho$ bringen lassen, kann man sie auf die Form $a_2+b_2\sigma$ bringen und nur mit Zahlen dieser Form rechnen. Weil aber die Operationen mit $a+b\varrho$ einfacher sind als die mit $a+b\sigma$, so werden wir diese Darstellung benutzen nur wenn $D = 4t+3$ ist (Satz 4, § 1), weil nicht alles, was für die Zahlen $a+b\varrho$ richtig ist, auch für die Zahlen $a+b\sigma$ richtig bleibt, so werden wir für diese beiden Formen die folgende Untersuchung parallel durchführen. In den allgemein gültigen Fällen werden wir statt $a+b\varrho$ und $a+b\sigma$ die Form $a+b\theta$ benutzen; θ ist also ϱ oder σ.

1) Satz 1 und 2 folgen auch aus den Eigenschaften einer Basis.

Wir nehmen an, es sei

$$N(a+b\theta) \geqq N(\alpha+\beta\theta) > 0. \tag{2}$$

Ist $\alpha+\beta\theta$ ein Teiler von $a+b\theta$, so ist, ebenso wie bei rationalen Zahlen, $\alpha+\beta\theta$ der gesuchte größte gemeinschaftliche Teiler; ist das nicht der Fall, so werden wir versuchen eine Gleichung zu bilden

$$a+b\theta = (\alpha+\beta\theta)(p+q\theta)+\mu+\nu\theta, \tag{3}$$

wo $p+q\theta$ und $\mu+\nu\theta$ ganz sind und

$$N(\mu+\nu\theta) < N(\alpha+\beta\theta)$$

ist und weil in der so gebildeten Gleichung

$$G(a+b\theta,\ \alpha+\beta\theta) = G(\alpha+\beta\theta,\ \mu+\nu\theta)$$

ist, so wird durch diese Gleichung die Anwendung des Euklidischen Algorithmus auch auf die zu untersuchenden Zahlen übertragen in dem Sinne, daß wir in dieser Weise so lange fortfahren, bis unter den sukzessiven Normen von $\mu+\nu\theta$, $\mu_1+\nu_1\theta, \ldots$ die Zahl 0 auftritt.

Ist die Möglichkeit da, die Normen dieser Zahlen beständig zu verkleinern, so muß der Nullwert notwendig nach einer endlichen Anzahl von Operationen eintreten, weil die Normen dieser Reste ganze rationale positive Zahlen sind (Satz 3, § 2), die beständig abnehmen.

Ist $\mu_t+\nu_t\theta$ der letzte von diesen Resten, welcher einen von 0 verschiedenen Wert hat, so haben wir eine Kette von Gleichungen von folgender Form

$$\begin{aligned}
a+b\theta &= (\alpha+\beta\theta)(p+q\theta)+\mu+\nu\theta\\
\alpha+\beta\theta &= (\mu+\nu\theta)(p_1+q_1\theta)+\mu_1+\nu_1\theta\\
\mu+\nu\theta &= (\mu_1+\nu_1\theta)(p_2+q_2\theta)+\mu_2+\nu_2\theta\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\\
\mu_{t-1}+\nu_{t-1}\theta &= (\mu_t+\nu_t\theta)(p_{t+1}+q_{t+1}\theta)
\end{aligned}$$

aus welcher hervorgeht, daß $\mu_t+\nu_t\theta$ der gemeinschaftliche Divisor von $a+b\theta$ und $\alpha+\beta\theta$ ist und umgekehrt jeder Divisor von $a+b\theta$ und $\alpha+\beta\theta$ notwendig ein Divisor von $\mu_t+\nu_t\theta$ ist. Die Zahl $\mu_t+\nu_t\theta$ und ebenso jede Zahl, welche sich von $\mu_t+\nu_t\theta$ durch einen Einheitsfaktor unterscheidet, ist also der größte gemeinschaftliche Teiler von $a+b\theta$ und $\alpha+\beta\theta$.

Ein von $\mu_t+\nu_t\theta$ verschiedener größter gemeinschaftlicher Teiler ist für die Zahlen $a+b\theta$ und $\alpha+\beta\theta$, wie wir gesehen haben, nicht zulässig.

Um die Gleichung (3) zu bilden, werden wir zuerst den folgenden Satz beweisen.

Satz 3: *Der Quotient* $\dfrac{a+b\theta}{\alpha+\beta\theta}$ *läßt sich auf die Form* $u+v\theta$ *bringen, in der* u *und* v *rationale Zahlen sind.*

Beweis: Ist $\theta = \varrho$, so multiplizieren wir Zähler und Nenner mit

$$\alpha - \beta\varrho.$$

Wir bekommen dann

$$\text{(C)} \qquad \frac{a+b\varrho}{\alpha+\beta\varrho} = u + v\varrho = \frac{a\alpha + Db\beta}{\alpha^2 + D\beta^2} + \frac{\alpha b - a\beta}{\alpha^2 + D\beta^2}\varrho$$

also

$$u = \frac{a\alpha + Db\beta}{\alpha^2 + D\beta^2} \quad \text{und} \quad v = \frac{\alpha b - a\beta}{\alpha^2 + D\beta^2}.$$

Damit ist der Satz für $\theta = \varrho$ bewiesen. Die Formel (4) werden wir als Formel der Division benutzen.

Ist $\theta = \sigma = \frac{x + y\varrho}{2}$, so multiplizieren wir Zähler und Nenner mit $\alpha + \beta\frac{x - y\varrho}{2}$, wir bekommen dann

$$\text{(1)} \qquad \frac{a+b\sigma}{\alpha+\beta\sigma} = \frac{4a(\alpha+\beta x) + \beta b(x^2 + Dy^2)}{\beta^2(x^2+Dy^2) + 4\alpha(\alpha+\beta x)} + \frac{4(\alpha b - a\beta)}{\beta^2(x^2+Dy^2) + 4\alpha(\alpha+\beta x)}\sigma,$$

also

$$u = \frac{4a(\alpha+\beta x) + \beta b(x^2+Dy^2)}{\beta^2(x^2+Dy^2) + 4\alpha(\alpha+\beta x)} \quad \text{und} \quad v = \frac{4(\alpha b - a\beta)}{\beta^2(x^2+Dy^2) + 4\alpha(\alpha+\beta x)}$$

q. e. d.

Setzen wir $u = p + \xi$ und $v = q + \eta$, wo p und q ganze Zahlen sind, so ist

$$\frac{a+b\theta}{\alpha+\beta\theta} = p + q\theta + \xi + \eta\theta.$$

Daraus folgt, daß

$$a + b\theta = (\alpha+\beta\theta)(p+q\theta) + (\alpha+\beta\theta)(\xi+\eta\theta).$$

Das Produkt $(\alpha+\beta\theta)(\xi+\eta\theta)$ ist offenbar eine ganze Zahl, weil

$$a + b\theta \quad \text{und} \quad (\alpha+\beta\theta)(p+q\theta)$$

ganz sind. Wir werden sie mit $\mu + \nu\theta$ bezeichnen.

Ist $\mu + \nu\theta = (\alpha+\beta\theta)(\xi+\eta\theta) = 0$, so ist $\alpha + \beta\theta$ der gesuchte größte gemeinschaftliche Teiler. In diesem Falle ist auch

$$N(\alpha+\beta\theta)N(\xi+\eta\theta) = 0.$$

Da aber $N(\alpha+\beta\theta) > 0$ ist, so muß dazu

$$N(\xi+\eta\theta) = 0$$

sein. Aus der Formel

$$\text{(6)} \qquad N(\mu+\nu\theta) = N(\alpha+\beta\theta)N(\xi+\eta\theta)$$

folgt unmittelbar:

Satz 4: *Die $N(\mu+\nu\theta)$ ist der $N(\xi+\eta\theta)$ proportional.*

Wir werden jetzt den folgenden Satz beweisen.

Satz 5: *$N(\xi+\eta\theta) = 0$ wird erfüllt, wenn $\xi = 0$ und $\eta = 0$ ist.*

Beweis: Ist $\theta = \varrho$, so ist dieser Satz schon bewiesen (Satz 4, § 2).

Ist $\theta = \sigma$, so ist

$$\xi + \eta\theta = \xi + \eta\,\frac{x + y\varrho}{2} = \left(\xi + \frac{\eta x}{2}\right) + \frac{\eta y}{2}\,\varrho = t + u\varrho.$$

Damit also $N(\xi + \eta\theta)$ wird, muß $N(t + u\varrho) = 0$ werden. Dazu muß (Satz 4, § 2) $t = 0$ und $u = 0$ werden. Da aber $u = \frac{\eta y}{2}$ und y von 0 verschieden ist, so muß $\eta = 0$ sein. Da $u = \xi + \frac{\eta x}{2}$ und $\eta = 0$ sein muß, so muß es auch ξ sein, q. e. d.

Aus der Formel (6) folgt auch der folgende Satz.

Satz 6: *Damit der Euklidische Algorithmus anwendbar wird, muß*

$$N(\xi + \eta\theta) < 1$$

sein und umgekehrt.

Beweis: Es soll

$$N(\mu + \nu\theta) = N(\alpha + \beta\theta)N(\xi + \eta\theta) < N(\alpha + \beta\theta)$$

sein, weil aber $N(\alpha + \beta\theta) > 0$ ist (Satz 3 § 2), so muß

$$N(\xi + \eta\theta) < 1 \tag{7}$$

sein. q. e. d.

Umgekehrt, wäre

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta,$$

wo

$$N(\mu + \nu\theta) < N(\alpha + \beta\theta)$$

ist, so ist

$$\frac{a + b\theta}{\alpha + \beta\theta} = p + q\theta + \frac{\mu + \nu\theta}{\alpha + \beta\theta};$$

setzen wir

$$\frac{\mu + \nu\theta}{\alpha + \beta\theta} = \xi + \eta\theta,$$

was immer möglich ist (Satz 3), so ist

$$\mu + \nu\theta = (\alpha + \beta\theta)(\xi + \eta\theta),$$

folglich

$$N(\mu + \nu\theta) = N(\alpha + \beta\theta)N(\xi + \eta\theta);$$

ist

$$N(\xi + \eta\theta) < 1,$$

so ist also

$$N(\mu + \nu\theta) < N(\alpha + \beta\theta),$$

q. e. d.

Diese Bedingung ist nicht nur notwendig, sondern auch hinreichend dafür, daß $N(\mu + \nu\theta) < N(\alpha + \beta\theta)$ werde.

Da $N(\xi + \eta\theta) \geqq 0$ ist (Satz 3 § 2), so ist der Wert 0 der möglichst kleinste für diese Norm. Ist $N(\xi + \eta\theta) \geqq 1$, so kann sie durch Verkleinerung < 1 werden. Ist $N(\xi + \eta\theta) < 1$, so bleibt sie auch kleiner als 1, wenn wir ihren Wert verkleinern, und wenn ihr Wert kleiner wird, so wird auch $N(\mu + \nu\theta)$ kleiner (Satz 4). Dadurch sind wir dem Ziele schon

näher. Es kommt also zuvörderst darauf an, die $N(\xi + \eta\theta)$ möglichst zu verkleinern. Wir werden dazu zuerst den folgenden Satz beweisen.

Satz 7: *Die Verkleinerung von $N(\xi + \eta\sigma)$ ist von der Wahl der Zahl σ unabhängig.*

Beweis: Es sei

$$a + b\sigma = (\alpha + \beta\sigma)(p + q\sigma) + (\alpha + \beta\sigma)(\xi + \eta\sigma).$$

Nehmen wir statt σ eine andere Zahl σ_1, so ist $a + b\sigma = a_1 + b_1\sigma_1$ und $\alpha + \beta\sigma = \alpha_1 + \beta_1\sigma_1$ (Satz 2). Wir nehmen an, daß jetzt eine neue Zerlegung

$$a_1 + b_1\sigma_1 = (\alpha_1 + \beta_1\sigma_1)(p_1 + q_1\sigma_1) + (\alpha_1 + \beta_1\sigma_1)(\xi_1 + \eta_1\sigma_1)$$

möglich ist, worin

$$N(\xi_1 + \eta_1\sigma_1) < N(\xi + \eta\sigma)$$

ist. Transformieren wir die in der letzten Gleichung vorkommenden Zahlen so, daß statt σ_1 wieder σ eintritt (Satz 2), dann ist

$$a + b\sigma = (\alpha + \beta\sigma)(p_2 + q_2\sigma) + (\alpha + \beta\sigma)(\xi_2 + \eta_2\sigma);$$

aus der Gleichung

$$\xi_1 + \eta_1\sigma_1 = \xi_2 + \eta_2\sigma$$

folgt aber

$$N(\xi_1 + \eta_1\sigma_1) = N(\xi_2 + \eta_2\sigma).$$

Ist also

$$N(\xi_1 + \eta_1\sigma_1) < N(\xi + \eta\sigma),$$

so ist dasselbe dadurch erreichbar, daß

$$N(\xi_2 + \eta_2\sigma) < N(\xi + \eta\sigma).$$

Ist also $N(\xi + \eta\sigma)$ dadurch verkleinert, daß wir σ_1 statt σ benutzen, so ist dies auch erreichbar für dasselbe σ durch Veränderung der Zahlen ξ und η.

Die Wahl der Zahl σ spielt also keine wesentliche Rolle, infolgedessen brauchen wir gebrochene x, y nicht zu berücksichtigen. Wir können sogar beliebige ganze Werte von x, y benutzen, welche nur die Bedingungen des Satzes 1 erfüllen. Wir werden infolgedessen $x = y = 1$ setzen. Diesen speziellen Wert von σ werden wir durch ϑ bezeichnen. Es ist also

$$\vartheta = \frac{1 + \varrho}{2}. \tag{8}$$

ϑ ist ganz, weil $\frac{1 + D}{4}$ ganz ist (Satz 4, § 1). Wir werden aus dieser Wahl der Zahl ϑ einige für uns wichtige Schlüsse ziehen.

Satz 8: *Die Zahl $a + b\vartheta$ ist eine ganze Zahl, wenn a und b irgend welche ganze rationale Zahlen sind.*

Beweis:

$$a + b\vartheta = a + b\frac{1 + \varrho}{2} = \frac{(2a + b) + b\varrho}{2}.$$

Damit diese Zahl ganz sein soll, muß

$$\frac{(2a+b)^2+Db^2}{4} = \frac{4a^2+4ab+b^2(1+D)}{4}$$

ganz sein (Satz 2, § 1). Weil aber $\frac{1+D}{4}$ ganz ist, so ist das für ganzzahlige a und b immer der Fall.

Satz 9: *Es ist*

$$\vartheta^2 = \vartheta - \frac{1+D}{4}. \tag{9}$$

Diese Formel ergibt sich durch einfache Rechnung.

Satz 10: *Es ist*

$$N(a+b\vartheta) = a^2 + b^2\frac{1+D}{4} + ab. \tag{10}$$

Satz 11: *Es ist*

$$\frac{a+b\vartheta}{\alpha+\beta\vartheta} = \frac{4a(\alpha+\beta)+\beta b(1+D)}{\beta^2(1+D)+4\alpha(\alpha+\beta)} + \frac{4(\alpha b-a\beta)}{\beta^2(1+D)+4\alpha(\alpha+\beta)}\vartheta. \tag{11}$$

Die letzten zwei Sätze ergeben sich unmittelbar, wenn wir $x = y = 1$ in die Formel (1) und (5) einsetzen.

Die Gleichung (11′) werden wir auch als Divisionsverfahren benutzen.

Wir brauchen jetzt die Zahlen ξ und η so zu wählen, daß $N(\xi+\eta\vartheta)$ bei diesen willkürlich angenommenen ϑ möglichst verkleinert wird, weil nur die ganzen Bestandteile von ξ und η willkürlich sind und die Stetigkeit gänzlich ausgeschlossen ist, so läßt sich dieser Minimalwert nur durch arithmetische Überlegungen erreichen.

Ist $D = 4t+1$ oder $= 2t$, so ist $\theta = \varrho$,

$$N(\xi+\eta\theta) = \xi^2 + D\eta^2 \quad ((1), \S\ 2)$$

und weil jeder Summand positiv ist, so wird diese Summe verkleinert, wenn ξ^2 oder η^2, also $|\xi|$ oder $|\eta|$ kleiner werden. Den möglichst kleinsten Wert bekommt also dieser Ausdruck, wenn $|\xi|$ und $|\eta|$ ihren kleinsten Wert erreichen. Das ist der Fall für $|\xi| \leqq \frac{1}{2}$ und $|\eta| \leqq \frac{1}{2}$.

Die Bedingung $N(\xi+\eta\varrho) > 1$ ist für $D = 1$ und $D = 2$, aber nur in diesen Fällen immer erreichbar, denn im ersten Fall ist

$$\xi^2 + D\eta^2 = \xi^2 + \eta^2 \leqq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

im zweiten

$$\xi^2 + D\eta^2 = \xi^2 + 2\eta^2 \leqq \tfrac{1}{4} + \tfrac{1}{2} = \tfrac{3}{4},$$

also

Satz 12: *Für den Gaußschen Körper $R(i)$ und für $R(\sqrt{-2})$ ist der Euklidische Algorithmus immer anwendbar.*

Beispiel: Es ist $G(1+13i,\ 7-4i)$ zu bestimmen.

$$\frac{1+13i}{7-4i} = \frac{-45}{65} + \frac{-95}{65}i = -1 + i + \frac{4}{13} + \frac{6}{13}i,$$

$$1+13i = (7-4i)(-1+i) + 4 + 2i,$$

$$\frac{7-4i}{4+2i} = \frac{20}{20} + \frac{-30}{20}i = 1 - i - \frac{1}{2}i,$$

$$7 - 4i = (4 + 2i)(1 - i) + 1 - 2i,$$

$$\frac{4+2i}{1-2i} = \frac{0}{5} + \frac{10}{5}i = 2i,$$

also

$$G(1 + 13i,\ 7 - 4i) = 1 - 2i.$$

Ist $D = 4t + 3$, so ist $\theta = \vartheta$ und nach (10)

$$N(\xi + \eta\vartheta) = \xi^2 + \eta^2\frac{1+D}{4} + \xi\eta.$$

Die Vorzeichen von ξ und η spielen also nur eine Rolle, insofern sie gleich oder verschieden sind. Wir können ξ und η als positive Zahlen betrachten und nur untersuchen für welche ξ und η die Zahl

$$N(\xi \pm \eta\vartheta) < 1$$

ist und den kleinsten Wert annimmt.

Es ist

$$\xi \pm \eta\vartheta = \xi \pm \frac{\eta}{2} \pm \frac{\eta}{2}\varrho$$

also ist

$$N(\xi \pm \eta\vartheta) = \left(\xi \pm \frac{\eta}{2}\right)^2 + \frac{\eta^2 D}{4}.$$

Weil aber $\frac{\eta^2 D}{4}$ und $\left(\xi \pm \frac{\eta}{2}\right)^2$ positive Zahlen sind, so brauchen wir $\left|\xi \pm \frac{\eta}{2}\right|$ und $|\eta|$ möglichst zu verkleinern, außerdem muß $\frac{\eta^2 D}{4} < 1$ und $\left(\xi \pm \frac{\eta}{2}\right)^2 < 1$ sein, d. h. erstens muß

$$(12)\quad \begin{cases} |\eta| < \frac{2}{\sqrt{D}}, \text{ also } |\eta| < 1{,}15 \text{ in } R(\sqrt{-3}), \quad |\eta| < 0{,}75 \text{ in } R(\sqrt{-7}), \\ |\eta| < 0{,}60 \text{ in } R(\sqrt{-11}) \quad \text{und} \quad |\eta| < 0{,}45 \end{cases}$$

in allen anderen zu untersuchenden Körpern sein, zweitens muß auch

$$\left|\xi \pm \frac{\eta}{2}\right| < 1$$

sein.

Setzen wir $\xi = \varkappa + \lambda$ und $\eta = \varkappa_1 + \lambda_1$, wo $\varkappa$ und $\varkappa_1$ positive ganze Zahlen, λ und λ_1 positive echte Brüche sind, so ist

$$\left|\xi \pm \frac{\eta}{2}\right| = \left|\left(\varkappa \pm \frac{\varkappa_1}{2}\right) + \left(\lambda \pm \frac{\lambda_1}{2}\right)\right|.$$

Daraus folgt, daß dieser Ausdruck in Bezug auf $\varkappa$ und $\varkappa_1$ den kleinsten Wert erreicht für $\varkappa \pm \frac{\varkappa_1}{2} = 0$, wenn $\lambda \pm \frac{\lambda_1}{2} \geqq 0$, was für $\lambda + \frac{\lambda_1}{2}$ immer der Fall ist, weil λ und λ_1 positive Zahlen sind. Ist $\lambda - \frac{\lambda_1}{2} < 0$, so ist $\lambda < \frac{\lambda_1}{2} < \frac{1}{2}$, weil λ_1 ein echter Bruch ist, also ist $\left|\lambda - \frac{\lambda_1}{2}\right| < \frac{1}{2}$. Ist in

diesem Fall $\left|\lambda - \frac{\lambda_1}{2}\right| < \frac{1}{4}$, so ist $\left|\xi - \frac{\eta}{2}\right| < \frac{1}{4}$ für $\varkappa - \frac{\varkappa_1}{2} = 0$, schon aber für $\varkappa - \frac{\varkappa_1}{2} = \frac{1}{2}$ ist

$$\left|\xi - \frac{\eta}{2}\right| > \frac{1}{4}$$

und der möglichst kleinste Wert in Bezug auf $\varkappa, \varkappa_1$ ist wieder erreicht, wenn $\varkappa - \frac{\varkappa_1}{2} = 0$ ist. Ist $\left|\lambda - \frac{\lambda_1}{2}\right| > \frac{1}{4}$, so ist der möglichst kleinste Wert erreicht, wenn $\varkappa - \frac{\varkappa_1}{2} = \frac{1}{2}$ ist.

Damit $\varkappa - \frac{\varkappa_1}{2} = 0$ wird, muß $\varkappa = \varkappa_1 = 0$ gewählt werden, denn ist $D > 11$, so ist nach (12) $\varkappa_1 = 0$, ist $D = 3$ oder 7 oder 11, so kann $\varkappa_1 = 1$ sein. Bei diesem Wert kann aber $\varkappa - \frac{\varkappa_1}{2}$ nicht 0 werden, $\varkappa - \frac{\varkappa_1}{2} = \frac{1}{2}$ ist nur möglich, wenn $\varkappa_1 = 1$, also auch $\varkappa = 1$ ist, also der Wert $\frac{1}{2}$ kommt nur in Betracht, wenn $D = 3$ oder 7 oder 11 ist. Wir werden beweisen, daß bei der Bedingung $\lambda - \frac{\lambda_1}{2} < 0$ und $D = 3$ oder 7 oder 11 auch $\varkappa - \frac{\varkappa_1}{2} = 0$ vorzuziehen ist, weil $N(\xi - \eta\vartheta)$ sich dadurch verkleinert, trotzdem $\left|\xi - \frac{\eta}{2}\right|$, d. h. ihr erster Bestandteil sich vergrößert.

Es ist zu beweisen, daß

$$\left(1 + \lambda - \frac{1 + \lambda_1}{2}\right)^2 + \frac{(1+\lambda_1)^2 \cdot D}{4} > \left(\lambda - \frac{\lambda_1}{2}\right)^2 + \frac{\lambda_1^2 \cdot D}{4}$$

oder

$$\left[\frac{1}{2} + \left(\lambda - \frac{\lambda_1}{2}\right)\right]^2 + \frac{(1+\lambda_1)^2 \cdot D}{4} > \left(\lambda - \frac{\lambda_1}{2}\right)^2 + \frac{\lambda_1^2 \cdot D}{4}$$

oder

$$\frac{1}{4} + \left(\lambda - \frac{\lambda_1}{2}\right) + \left(\lambda - \frac{\lambda_1}{2}\right)^2 + \frac{D}{4} + \frac{D\lambda_1}{2} + \frac{D\lambda_1^2}{4} > \left(\lambda - \frac{\lambda_1}{2}\right)^2 + \frac{D\lambda_1^2}{4}$$

oder

$$\frac{1}{4} + \lambda + \frac{\lambda_1}{2}(D-1) + \frac{D}{4} > 0.$$

Diese letzte Ungleichung ist aber richtig, da $D - 1 > 0$ ist, und alle Summanden in der linken Seite dieser Ungleichung positive Zahlen sind. Es ist also $|\xi| = |\lambda|$ und $|\eta| = |\lambda_1|$.

Setzen wir $|h| \leqq \frac{1}{2}$ und $|h_1| \leqq \frac{1}{2}$, so kann $\lambda = +h$ oder $-(1-h)$ sein, $\lambda_1 = \pm h_1$ oder $\mp(1 - h_1)$ sein. Es ist noch zu unterscheiden, welcher von diesen Werten vorzuziehen ist.

Aus den Ungleichungen (12) folgt zuerst, daß wir nur dann zwischen $\pm h_1$ und $\mp(1 - h_1)$ zu unterscheiden haben, wenn $D = 3$ oder 7 oder 11 ist, für alle anderen D kommt nur $\pm h_1$ in Betracht, ob h oder $-(1-h)$ vorzuziehen ist, läßt sich durch ein einfaches Kriterium angeben, es ist nämlich

$$N(h \pm h_1\vartheta) - N[-(1-h) \pm h_1\vartheta] = -(1-2h) \pm h_1.$$

Die Zahl $-(1-2h) - h_1$ ist negativ, weil $h < \frac{1}{2}$ ist, daraus folgt, daß, wenn wir h und $-h_1$ haben $h - h_1\vartheta$ vorzuziehen ist. Haben wir h und h_1, so ist $h + h_1\vartheta$ vorzuziehen, wenn

$$h_1 > 1 - 2h \tag{13}$$

ist. Im entgegengesetzten Fall ist $-(1-h) + h_1\vartheta$ vorzuziehen.

Wir werden auch für $D = 3$ oder 7 und 11 nur h_1 benutzen und beweisen den

Satz 13: *Für die Körper* $R(\sqrt{-3})$, $R(\sqrt{-7})$ und $R(\sqrt{-11})$ *ist der Euklidische Algorithmus immer anwendbar.*

Ist $D = 3$, so ist

$$N(h \pm h_1\vartheta) = h^2 \pm hh_1 + h_1^2 \leqq \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{3}{4}.$$

Ist $D = 7$, so ist

$$N(h \pm h_1\vartheta) = h^2 \pm hh_1 + 2h_1^2.$$

Haben wir mit dem Fall $h - h_1\vartheta$ zu tun, so ist

$$h^2 - hh_1 + 2h_1^2 \leqq \tfrac{1}{4} + \tfrac{2}{4} = \tfrac{3}{4},$$

haben wir mit dem Fall $h + h_1\vartheta$ zu tun und ist $h < \frac{1}{2}$ oder $h_1 < \frac{1}{2}$, so ist

$$h^2 + hh_1 + 2h_1^2 < \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{2}{4} = 1,$$

in dem Grenzfall $h = \frac{1}{2}$ und $h_1 = \frac{1}{2}$ wird die Ungleichung (11) erfüllt, wir können also eine normkleinere Zahl bekommen, wenn wir statt h die Zahl $-(1-h)$, d. h. $-\frac{1}{2}$ wählen. Tun wir das, so wird

$$N(-\tfrac{1}{2} + \tfrac{1}{2}\vartheta) = \tfrac{1}{4} - \tfrac{1}{4} + \tfrac{1}{2} = \tfrac{1}{2}$$

also wieder < 1.

Ist $D = 11$, so läßt sich die Anwendbarkeit des Euklidischen Algorithmus folgendermaßen beweisen.

Haben wir mit dem Fall $h - h_1\vartheta$ zu tun, so ist

$$N(h - h_1\vartheta) = h^2 - hh_1 + 3h_1^2 < h^2 + 3h_1^2 < \tfrac{1}{4} + \tfrac{3}{4} = 1.$$

Haben wir mit dem Fall $h + h_1\vartheta$ zu tun, so ist

$$N(h + h_1\vartheta) = h^2 + hh_1 + 3h_1^2 < \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{3}{4} = \tfrac{5}{4} \tag{14}$$

also kann auch $N(h + h_1\vartheta) \geqq 1$ sein. Wir werden beweisen, daß in diesem Fall statt h die Zahl $-(1-h)$ zu wählen ist, denn dadurch wird

$$N(-(1-h) + h_1\theta) < 1$$

und der Euklidische Algorithmus ist wieder anwendbar.

In der Tat, in diesem Fall ist

$$N(h + h_1\theta) = h^2 + hh_1 + 3h_1^2 = 1 + t,$$

wo nach (14) $t < \frac{1}{4}$ ist.

Es ist also

$$h = -\frac{h_1}{2} + \sqrt{\frac{h_1^2}{4} - 3h_1^2 + 1 + t}.$$

Dem entsprechend ist

$$N(-(1-h) + h_1\theta) = (1-h)^2 - (1-h)h_1 + 3h_1^2 = 1 - 2h - h_1 + 1 + t$$

$$= 2 + t - 2\sqrt{\frac{h_1^2}{4} - 3h_1^2 + 1 + t} = 2 + t - \sqrt{4(1+t) - 11h_1^2}.$$

Damit $N(-(1-h) + h_1\theta) < 1$ sein soll, muß

$$2 + t - \sqrt{4(1+t) - 11h_1^2} < 1$$

sein, also muß

$$1 + t < \sqrt{4(1+t) - 11h_1^2}$$

sein, oder

$$(1+t)^2 < 4(1+t) - 11h_1^2$$

und weiter

$$11h_1^2 < 3 + (2t - t^2). \tag{15}$$

Aus der Ungleichung $t < \frac{1}{4}$ folgt, daß

$$2t - t^2 > 0$$

ist, also wird die Ungleichung (15) erfüllt, wenn

$$11h_1^2 < 3$$

ist. Diese Ungleichung ist aber erfüllt, da $h_1 \leqq \frac{1}{2}$ ist. Demnach

Satz 14: *Für $D = 3$ und $D = 7$ ist $|\xi| < \frac{1}{2}$, $|\eta| < \frac{1}{2}$, für $D > 7$ ist $|\xi| < 1$, $|\eta| < \frac{1}{2}$.* Die Zahl ξ wird $= -(1-h)$ *gewählt, nur wenn wir mit $-h_1$ zu tun haben und $h_1 > 1 - 2h$ ist.*

Aus der Bedingung $|\eta| < \frac{2}{\sqrt{D}}$ folgt, daß die Ungleichung

$$N(\xi + \eta\vartheta) < 1$$

für $D > 11$ nicht immer erreichbar ist. Es kann nämlich

$$\frac{2}{\sqrt{D}} < |\eta| < \frac{1}{2} \tag{16}$$

sein.

Solche Beispiele lassen sich leicht auf verschiedenem Wege finden, z. B. durch Auflösung zweier Diophantischen Gleichungen

$$a = \alpha u - \beta v\,\frac{1+D}{4},$$

$$b = \beta(u+v) + \alpha v$$

mit drei Unbekannten. Diese Gleichungen erhalten wir bei entsprechender Wahl der Zahl u, willkürlichem v und willkürlichem ganzzahligem Wert einer der Zahlen a, b, α, β in der Gleichung

$$\frac{a+b\theta}{\alpha+\beta\theta} = u + v\theta.$$

Als Beispiel kann man auch immer die Zahlen $a + \varrho$ und 2 benutzen.

Ist in der angegebenen Weise die Ungleichung

$$N(\xi + \eta\theta) < 1$$

erreichbar, so kommen wir durch Verkleinerung der $N(\mu + \nu\theta)$ entweder zu $N(\mu + \nu\theta) = 1$ oder $= 0$. Im ersten Fall haben $a + b\theta$ und $\alpha + \beta\theta$ keine gemeinschaftlichen Faktoren außer den Einheiten, im zweiten finden wir einen größten gemeinschaftlichen Teiler. Ist

$$N(\xi + \eta\theta) \geqq 1,$$

so wird in der Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$
$$N(\mu + \nu\theta) > N(\alpha + \beta\theta)$$

und der Euklidische Algorithmus ist nicht anwendbar; es kann aber der Fall sein, daß

$$N(\mu + \nu\theta) < N(a + b\theta),$$

d. h. diese neue Zahl $\mu + \nu\theta$ ist normkleiner als die normgrößere unter den gegebenen, ohne notwendigerweise auch normkleiner zu sein, als die normkleinere Zahl.

Wir kommen in diesem Fall auf die Frage, ob sich vielleicht der Euklidische Algorithmus auch in diesem Fall anwenden läßt, wenn auch in einem beschränkten Sinne, nämlich, daß statt $a + b\theta$ die Zahl $\mu + \nu\theta$ eingeführt wird, deren Norm kleiner ist, und ob sich vielleicht die Aufgabe $G(a + b\theta, \alpha + \beta\theta)$ zu finden auf die Auffindung von $G(\alpha + \beta\theta, \mu + \nu\theta)$, wo die Norm der einen Zahl verkleinert ist, reduzieren läßt.

Merkwürdigerweise stellt sich heraus, daß diese Frage mit nein beantwortet werden muß. Ist nämlich $N(\mu + \nu\theta) > N(\alpha + \beta\theta)$, so ist der Euklidische Algorithmus auch in diesem beschränkten Sinne nicht anwendbar. Sonst müßte es möglich sein nach der Gleichung

(3) $$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$

noch die Gleichung

$$\mu + \nu\theta = (\alpha + \beta\theta)(p_1 + q_1\theta) + \mu_1 + \nu_1\theta,$$

wo

(17) $$N(\mu + \nu\theta) > N(\mu_1 + \nu_1\theta)$$

ist, zu bilden. In diesem Fall wird

$$a + b\theta = (\alpha + \beta\theta)[(p + p_1) + (q + q_1)\theta] + \mu_1 + \nu_1\theta.$$

Weil aber

$$N(\mu + \nu\theta) = N(\alpha + \beta\theta)N(\xi + \eta\theta)$$

und

$$N(\mu_1 + \nu_1\theta) = N(\alpha + \beta\theta)N(\xi_1 + \eta_1\theta),$$

so muß, damit die Ungleichung (17) erfüllt wird,

$$N(\xi_1 + \eta_1\theta) < N(\xi + \eta\theta)$$

sein, was unmöglich ist, da in der Gleichung (3) ξ und η so gewählt sind, daß $N(\xi + \eta\theta)$ den möglichst kleinsten Wert angenommen hat.

Es ist nun noch die Frage zu beantworten, ob wir nicht auch in dem Fall

$$N(\mu + \nu\theta) > N(\alpha + \beta\theta)$$

durch weitere Division zum Ziel kommen, d. h. ob es vielleicht möglich ist, daß in der Gleichung

$$(3) \qquad a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$
$$N(\mu + \nu\theta) > N(\alpha + \beta\theta);$$

es lassen sich aber die weiteren Gleichungen

$$(18) \qquad \begin{cases} \mu + \nu\theta = (\alpha + \beta\theta)(p_1 + q_1\theta) + \mu_1 + \nu_1\theta \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mu_{h-1} + \nu_{h-1}\theta = (\alpha + \beta\theta)(p_h + q_h\theta) + \mu_h + \nu_h\theta \end{cases}$$

so lange bilden, bis wir endlich doch zum Fall

$$N(\mu_h + \nu_h\theta) < N(\alpha + \beta\theta)$$

kommen. Diese Frage muß auch mit nein beantwortet werden. Sonst bekommen wir aus den Gleichungen (3), (18) die folgende Gleichung

$$a + b\theta = (\alpha + \beta\theta)[(p + p_1 + \cdots + p_h) + (q + q_1 + \cdots + q_h)\theta] + \mu_h + \nu_h\theta.$$

Ist

$$N(\mu_h + \nu_h\theta) < N(\alpha + \beta\theta),$$

so folgt aus der Gleichung

$$N(\mu_h + \nu_h\theta) = N(\alpha + \beta\theta)N(\xi_h + \eta_h\theta),$$

daß

$$N(\xi_h + \eta_h\theta) < 1;$$

das ist aber unmöglich; denn sonst kann nicht in

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$

$N(\xi + \eta\theta)$ der möglichst kleinste Wert sein, weil

$$N(\xi + \eta\theta) > 1$$

ist.

Wir haben den Euklidischen Algorithmus anzuwenden versucht durch die Bildung der Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta,$$

und dazu haben wir $a + b\theta$ durch $\alpha + \beta\theta$ dividiert. Ist

$$N(\mu + \nu\theta) > N(\alpha + \beta\theta),$$

so ist noch die Frage zu erledigen, ob sich der Euklidische Algorithmus

nicht durch Division von $\alpha + \beta\theta$ durch $a + b\theta$ anwenden läßt, d. h. ob sich nicht durch die Bildung einer Gleichung

$$\alpha + \beta\theta = (a + b\theta)(p_1 + q_1\theta) + \mu_1 + \nu_1\theta, \tag{19}$$

wo $N(\mu_1 + \nu_1\theta) < N(\alpha + \beta\theta)$ ist, die Auffindung von $G(a + b\theta,\ \alpha + \beta\theta)$ auf die Auffindung von $G(\alpha + \beta\theta,\ \mu_1 + \nu_1\theta)$, wo $N(\mu_1 + \nu_1\theta) < N(\alpha + \beta\theta)$ ist, durch die Gleichung (19) notwendiger Weise zurückführen läßt?

Diese Frage muß auch mit nein beantwortet werden, denn aus der Ungleichung oder Gleichung

$$N(a + b\theta) \geqq N(\alpha + \beta\theta)$$

folgt, daß

$$N\left(\frac{\alpha + \beta\theta}{a + b\theta}\right) = N(u + v\theta) < 1$$

ist, also müssen u und v die Bedingungen erfüllen, welche in der Ungleichung (12) für ξ und η bestimmt sind, d. h. es ist $|u| < 1$ und $|v| < \frac{1}{2}$, infolgedessen kann in der Gleichung (19) p_1 nur die Werte 0 und ± 1 haben, q_1 aber nur den Wert 0. Ist $p_1 = 0$, so bekommt die Gleichung (19) die Form

$$\alpha + \beta\theta = \mu_1 + \nu_1\theta$$

und es ist dadurch nichts erreicht. Ist $p_1 = \pm 1$, so bekommt die Gleichung (19) die Form

$$\alpha + \beta\theta = \pm(a + b\theta) + \mu_1 + \nu_1\theta,$$

also ist

$$N(\mu_1 + \nu_1\theta) = (\alpha \pm a)^2 + (\beta \pm b)^2\,\frac{1 + D}{4} + (\alpha \pm a)(\beta \pm b).$$

Dabei muß

$$N(\mu_1 + \nu_1\theta) \leqq N(\alpha + \beta\theta)$$

sein, also ist

$$N(\mu_1 + \nu_1\theta) < N(\mu + \nu\theta),$$

daß ist aber unmöglich, denn setzen wir in (3) $p = +1$ oder -1, $q = 0$, so bekommen wir

$$N(\mu + \nu\theta) = N(\mu_1 + \nu_1\theta).$$

$\mu + \nu\theta$ in (3) ist aber die normkleinste Zahl und ihre Norm kann also nicht durch entsprechende Wahl von p und q verkleinert werden.

Aus diesen Überlegungen folgt:

Satz 15: *Der Euklidische Algorithmus kann nicht für die quadratischen imaginären Zahlen in irgend einem Sinn verändert werden.*

Die Ungleichung, eventuell Gleichung,

$$N(\xi + \eta\theta) \geqq 1$$

ist, wie gezeigt, in jedem zu untersuchenden Körper $R(\sqrt{-D})$ und $D > 11$ möglich. Es kann also von einer allgemeinen Anwendung des Euklidischen Algorithmus mit Ausnahme von $R(\sqrt{-1})$, $R(\sqrt{-2})$,

$R(\sqrt{-3})$, $R(\sqrt{-7})$ und $R(\sqrt{-11})$ für keinen einzelnen von den zu untersuchenden Körpern die Rede sein. In jedem dieser Körper kann er nur für einzelne Zahlen Anwendung finden, um den größten gemeinschaftlichen Teiler wirklich zu finden oder mindestens die Zahlen $a + b\theta$ und $\alpha + \beta\theta$ auf normkleinere Zahlen zurückzuführen.

Somit haben wir auch bewiesen, daß der Satz: Ist der Euklidische Algorithmus anwendbar, so ist die Zerlegung in unzerlegbare Faktoren eindeutig,[1]) nicht umkehrbar ist, und wir können folgenden Satz aufstellen.

Satz 13: *Die eindeutige Zerlegung in unzerlegbare Faktoren ist keine Bedingung für die Anwendbarkeit des Euklidischen Algorithmus.*

Es ist von Interesse sagen zu können, ob der Euklidische Algorithmus versagt oder angewandt werden kann, bevor die Division ausgeführt worden ist. Ein solches allgemeines Kriterium ist aber unmöglich, wie sich folgendermaßen ergibt.

Aus der Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$

folgt

$$\mu + \nu\theta = (\alpha + \beta\theta)(\xi + \eta\theta),$$

also

$$N(a + b\theta) = N(\alpha + \beta\theta)N[(p + \xi) + (q + \eta)\theta];$$

wenn

$$N(\mu + \nu\theta) < N(\alpha + \beta\theta),$$

so ist auch

$$N(\mu + \nu\theta) < N(a + b\theta),$$

also ist

$$N(\mu + \nu\theta) < N(\alpha + \beta\theta)N[(p + \xi) + (q + \eta)\theta],$$

d. h.

$$N(\alpha + \beta\theta)N(\xi + \eta\theta) < N(\alpha + \beta\theta)N[(p + \xi) + (q + \eta)\theta]$$

oder weil

$$N(\alpha + \beta\theta) > 0,$$

so bekommen wir schließlich

$$N(\xi + \eta\theta) < N[(p + \xi) + (q + \eta)\theta]. \tag{20}$$

Ist $\theta = \varrho$, so folgt aus der letzten Gleichung

$$\xi^2 + D\eta^2 < (p + \xi)^2 + D(q + \eta)^2;$$

daraus folgt:

$$p^2 + Dq^2 + 2p\xi + 2Dq\eta > 0$$

und schließlich

$$(p^2 + 2p\xi) + D(q^2 + 2q\eta) > 0. \tag{21}$$

Ist $\theta = \vartheta$, so folgt aus der Ungleichung (20)

---

1) R. Dedekind „Vorlesungen über Zahlentheorie von L. Dirichlet“ § 159, p. 450. J. Sommer „Vorlesungen über Zahlentheorie“ § 7, p. 29.

$$\xi^2+\eta^2\,\frac{1+D}{4}+\xi\eta<(p+\xi)^2+(q+\eta)^2\,\frac{1+D}{4}+(p+\xi)(q+\eta)$$

was sich auf die Form

$$(22)\qquad (p^2+2p\xi)+(q^2+2q\eta)\,\frac{1+D}{4}+(pq+q\xi+p\eta)>0$$

bringen läßt.

Ist der Euklidische Algorithmus anwendbar, so müssen die Ungleichungen (21) und (22) entsprechend erfüllt sein; weil aber diese von p, q, ξ und η abhängig sind, so gehören zu einem solchen Kriterium alle diese Zahlen; diese können aber nur durch Division bestimmt werden. Ist aber die Division ausgeführt, so haben wir, wie gezeigt, ein einfaches Kriterium der Anwendbarkeit des Euklidischen Algorithmus in der Ungleichung

$$N(\xi+\eta\theta)<1.$$

Aus den Ungleichungen (21) und (22) läßt sich ein Kriterium angeben, wann dieses Versagen von p und q abhängig ist. Diese Ungleichungen versagen nämlich sobald p und q zugleich 0 sind.

Der Fall $p=0$ und $q=0$ ist ein ganz merkwürdiger. Bei dieser Voraussetzung ergibt sich

$$(23)\quad |\xi|=\left|\frac{a\alpha+Db\beta}{\alpha^2+D\beta^2}\right|\leqq\tfrac{1}{2}\text{ oder }|\xi|=\left|\frac{4a(\alpha+\beta)+\beta b(1+D)}{\beta^2(1+D)+4\alpha(\alpha+\beta)}\right|<1$$

und oder $<\frac{1}{2}$

$$(24)\quad |\eta|=\left|\frac{\alpha b-a\beta}{\alpha^2+D\beta^2}\right|\leqq\tfrac{1}{2}\text{ oder }|\eta|=\left|\frac{4(\alpha b-a\beta)}{\beta^2(1+D)+4\alpha(\alpha+\beta)}\right|<\tfrac{1}{2}.$$

Dabei ist noch vorausgesetzt, daß

$$(2)\quad a^2+Db^2\geqq\alpha^2+D\beta^2\text{ oder }a^2+b^2\,\frac{1+D}{4}+ab>\alpha^2+\beta^2\,\frac{1+D}{4}+\alpha\beta.$$

Drei Ungleichungen eventuell auch Gleichungen (23), (24) und (2) für vier Zahlen a, b, α, β bieten die Möglichkeit, zwei von diesen Zahlen, sagen wir a und b oder α und β zu eliminieren, und wir bekommen eine Relation zwischen a und b oder α und β in der Form einer Gleichung oder Ungleichung. Daraus folgt der Satz:

Satz 17: *Wenn etwa in $\alpha+\beta\theta$ die Zahlen α und β eine gewisse Relation erfüllen, so versagt der Euklidische Algorithmus — auf $a+b\theta$ und $\alpha+\beta\theta$ angewandt — bei allen noch möglichen Zahlen $a+b\theta$; oder wenn entsprechend in $a+b\theta$ die Zahlen a und b einer bestimmten Relation genügen, versagt der Algorithmus auch bei beliebigen $\alpha+\beta\theta$.*

Da diese Relation in komplizierter Form erscheint, und als Kriterium unnützlich bleibt, so werden wir auf sie nicht näher eingehen. Es ist aber von Interesse im voraus sagen zu können, wann der Fall $p=0$, $q=0$ eintreten wird. Es läßt sich dafür ein einfaches Kriterium angeben.

Aus den Gleichungen

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + (\alpha + \beta\theta)(\xi + \eta\theta)$$

und

$$p = 0,\ q = 0$$

folgt

$$N(a + b\theta) = N(\alpha + \beta\theta)N(\xi + \eta\theta) \text{ also } N(\xi + \eta\theta) \geqq 1.$$

Ist $\theta = \varrho$, so ist $N(\xi + \eta\theta) = \xi^2 + D\eta^2 \leqq \frac{1}{4} + \frac{1}{4}D = \frac{1}{4}(1 + D)$ folglich ist

$$4N(a + b\theta) \leqq (1 + D)N(\alpha + \beta\theta). \tag{25}$$

Ist $\theta = \vartheta$, so ist

$$N(\xi + \eta\vartheta) = \xi^2 + \eta^2\,\frac{1 + D}{4} + \xi\eta < 1 + \tfrac{1}{4}\cdot\frac{1 + D}{4} + \tfrac{1}{2} = \frac{25 + D}{16}$$

also ist

$$16N(a + b\vartheta) \leqq (25 + D)N(\alpha + \beta\vartheta). \tag{26}$$

Diese Ungleichungen, eventuell Gleichungen, sind Kennzeichen dafür, daß der Euklidische Algorithmus versagt. Daneben besteht noch die Bedingung

$$N(a + b\theta) \geqq N(\alpha + \beta\theta). \tag{2}$$

Es lassen sich aus diesen Ungleichungen eventuell Gleichungen für einzelne Körper noch verschiedene Schlüsse ziehen, auf die wir nicht näher eingehen. Wenn auch (25), (26) nicht erfüllt sind, kann, wie wir gesehen haben, doch der Euklidische Algorithmus versagen; denn die Ungleichung

$$N(\xi + \eta\theta) < 1 \tag{7}$$

braucht trotzdem nicht erfüllt zu sein und wenn diese Ungleichung in der angegebenen Weise nicht erfüllt werden kann, so ist die Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta \tag{3}$$

überhaupt nicht erfüllbar, und der Euklidische Algorithmus versagt vollständig.

Beispiel I: Es soll $G(8 + 3\sqrt{-3},\ -1 + 4\sqrt{-3})$ gefunden werden

$$N(8 + 3\sqrt{-3}) > N(-1 + 4\sqrt{-3}),$$

$$8 + 3\sqrt{-3} = 5 + 6\vartheta,\ -1 + 4\sqrt{-3} = -5 + 8\vartheta,$$

$$\vartheta = \frac{1 + \sqrt{-3}}{2},\ \vartheta^2 = \vartheta - 1$$

$$\frac{5 + 6\vartheta}{-5 + 8\vartheta} = \frac{63}{49} - \frac{70}{49}\vartheta = 1 - \vartheta + \frac{2}{7} - \frac{3}{7}\vartheta$$

$$(\tfrac{2}{7} - \tfrac{3}{7}\vartheta)(-5 + 8\vartheta) = 2 + \vartheta$$

$$5 + 6\vartheta = (-5 + 8\vartheta)(1 - \vartheta) + (2 + \vartheta)$$

$$\frac{-5 + 8\vartheta}{2 + \vartheta} = -\frac{7}{7} + \frac{21}{7}\vartheta = -1 + 3\vartheta$$

also ist

$$9(8+3\sqrt{-3},\ -1+4\sqrt{-3}) = 2+\vartheta = \frac{5+\sqrt{-3}}{2}.$$

Weil aber in $R(\sqrt{-3})$ sechs Einheiten nämlich

$$\pm 1,\ \pm\frac{-1+\sqrt{-3}}{2},\ \pm\frac{-1-\sqrt{-3}}{2}$$

vorhanden sind, so hat $G(8+3\sqrt{-3},\ -1+4\sqrt{-3})$ folgende 6 Werte

$$+(2-\sqrt{-3}),\ +\frac{5+\sqrt{-3}}{2},\ +\frac{1+3\sqrt{-3}}{2},$$

welche durch Multiplikation von dem gefundenen Wert $2-\sqrt{-3}$ mit diesen 6 Einheiten des Körpers $R(\sqrt{-3})$ erhalten werden.

Die Zerlegungen der Zahlen $-1+4\sqrt{-3}$ und $8+3\sqrt{-3}$, nämlich

$$-1+4\sqrt{-3} = (2-\sqrt{-3})(-2+\sqrt{-3}) = -(2-\sqrt{-3})^2 = \frac{5+\sqrt{-3}}{2}\cdot\frac{1+3\sqrt{-3}}{2}$$

und

$$8+3\sqrt{-3} = (2-\sqrt{-3})(1+2\sqrt{-3}) = \frac{5+\sqrt{-3}}{2}\cdot\frac{7+\sqrt{-3}}{2} = \frac{1+3\sqrt{-3}}{2}\cdot\frac{5-\sqrt{-3}}{2}$$

sind jedoch nicht mehrdeutige, sondern eindeutige

Beispiel II: Es ist $G\left(\frac{13+\sqrt{-19}}{2},\ \frac{5+\sqrt{-19}}{2}\right)$ zu bestimmen

$$\frac{13+\sqrt{-19}}{2} = 6+\vartheta,\ \frac{3+\sqrt{-19}}{2} = 2+\vartheta,\ \vartheta = \frac{1+\sqrt{-19}}{2},\ \vartheta^2 = \vartheta - 5$$

$$N(6+\vartheta) > N(2+\vartheta)$$

$$\frac{6+\vartheta}{2+\vartheta} = \frac{23}{11} - \frac{4}{11}\vartheta = 2 + \frac{1}{11} - \frac{4}{11}\vartheta$$

$$N\left(\frac{1}{11} - \frac{4}{11}\vartheta\right) < 1;\ \left(\frac{1}{11} - \frac{4}{11}\vartheta\right)(2+\vartheta) = 2-\vartheta;$$

$$6+\vartheta = 2(2+\vartheta)+2-\vartheta;\ \frac{2+\vartheta}{2-\vartheta} = \frac{3}{7} + \frac{4}{7}\vartheta = \vartheta - \frac{3}{7} - \frac{3}{7}\vartheta = \vartheta - 1 + \frac{4}{7} - \frac{3}{7}\vartheta$$

$$N\left(\frac{3}{7} + \frac{3}{7}\vartheta\right) > 1,\ \frac{3}{7} > 1 - \frac{6}{7},\ N\left(\frac{4}{7} - \frac{3}{7}\vartheta\right) = 1.$$

Die normkleinste Zahl $\xi+\eta\vartheta$ hat die Norm 1. Es muß aber $N(\xi+\eta\vartheta) < 1$ sein. Hier versagt der Euklidische Algorithmus.

In derartigen Fällen müssen wir uns demnach nach einem dem Prinzipe nach von dem Euklidischen verschiedenen Algorithmus umsehen.

Die Aufsuchung des größten gemeinschaftlichen Teilers von $a + b\theta$ und $\alpha + \beta\theta$ ließe sich bekanntlich auch durch Zerlegung dieser Zahlen in unzerlegbare Faktoren finden. Diese Zerlegung ist aber im Vergleich mit der Auffindung des größten gemeinschaftlichen Teilers, so lange wir in demselben Körper bleiben, in gewissem Sinne eine Aufgabe höherer Ordnung als letztere. Im folgenden wird sich aber ergeben, daß der größte gemeinschaftliche Teiler von $a + b\theta$ und $\alpha + \beta\theta$ immer gefunden werden kann durch Zerlegung in Primfaktoren von zwei ganzen rationalen Zahlen und durch eine endliche Anzahl von Operationen.

§ 4. Die Bestimmung des größten gemeinschaftlichen Teilers für eindeutig zerlegbare quadratische imaginäre Zahlen mittels der Normen dieser Zahlen.

Wir nehmen an, es sei

$$(1) \qquad m + n\varrho = (m_1 + n_1\varrho)(z + w\varrho)$$

$$(2) \qquad r + s\varrho = (r_1 + s_1\varrho)(z + w\varrho),$$

wo $m + n\varrho$, $r + s\varrho$, ..., $z + w\varrho$ ganze quadratische imaginäre Zahlen sein sollen, $m, n, \ldots, z, w$ sind also ganze rationale Zahlen oder die Hälften von ganzen rationalen Zahlen, ϱ sei $= \sqrt{-D}$, ferner sei $z + w\varrho$ der größte gemeinschaftliche Teiler von $m + n\varrho$ und $r + s\varrho$. Damit ist aber auch

$$N(m + n\varrho) = N(m_1 + n_1\varrho)\, N(z + w\varrho),$$

$$N(r + s\varrho) = N(r_1 + s_1\varrho)\, N(z + w\varrho),$$

oder

$$m^2 + Dn^2 = (m_1^2 + Dn_1^2)(z^2 + Dw^2),$$

$$r^2 + Ds^2 = (r_1^2 + Ds_1^2)(z^2 + Dw^2),$$

d. h. $z^2 + Dw^2$ ist immer ein Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$. Diese Zahlen und auch ihr Teiler $z^2 + Dw^2$ sind ganze rationale Zahlen (Satz 3, § 2). Aus den letzten Gleichungen folgt, daß z, w eine Gleichung erfüllen

$$z^2 + Dw^2 = k_h,$$

wo k_h ein gemeinschaftlicher Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$ ist. Setzen wir $z + w\varrho = x + y\varrho$ oder $\frac{x + y\varrho}{2}$, so ist x, y ein ganzzahliges Lösungspaar einer der beiden Gleichungen

$$(3) \qquad x^2 + Dy^2 = k_h \text{ oder } x^2 + Dy^2 = 4k_h.$$

Aber nicht umgekehrt: nicht jedes Lösungspaar einer derartigen Gleichung bietet einen Teiler der Zahlen $m + n\varrho$ und $r + s\varrho$. Dies und ferner auch die Zahl k_h erkennen wir folgendermaßen.

Es sei k der größte gemeinschaftliche Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$.

Wir bezeichnen alle Teiler von k, der abnehmenden Größe nach geordnet, durch $k_1, k_2, \ldots$ dann bilden alle gemeinschaftlichen Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$ eine endliche Reihe von Zahlen

(4) $$k, k_1, k_2, \ldots, k_{t-1}, 1.$$

Eine beliebige von ihnen werden wir mit k_h bezeichnen.

Die Zahlen $m_1 + n_1\varrho$ und $r_1 + s_1\varrho$ in den Gleichungen (1) und (2) sind nach Voraussetzung teilerfremd. Es ist aber möglich, daß jede dieser Zahlen sich noch in zwei Faktoren zerlegen läßt, von denen die einen gleiche Norm haben, d. h. daraus daß $m_1 + n_1\varrho$ und $r_1 + s_1\varrho$ teilerfremd sind, folgt noch nicht, daß $N(m_1 + n_1\varrho)$ und $N(r_1 + s_1\varrho)$ es sind, z. B. 3 und $\frac{1+\sqrt{-11}}{2}$ haben sogar dieselbe Norm 9, sind aber teilerfremd.

Nehmen wir also an, es sei

$$m_1 + n_1\varrho = (m_2 + n_2\varrho)(z_1 + w_1\varrho);\ r_1 + s_1\varrho = (r_2 + s_2\varrho)(z_2 + w_2\varrho)$$

wo

$$z_1^2 + Dw_1^2 = z_2^2 + Dw_2^2.$$

Dann ist

$$m + n\varrho = (m_2 + n_2\varrho)(z_1 + w_1\varrho)(z + w\varrho) = (m_2 + n_2\varrho)(z_3 + w_3\varrho)$$

und

$$r + s\varrho = (r_2 + s_2\varrho)(z_2 + w_2\varrho)(z + w\varrho) = (r_2 + s_2\varrho)(z_4 + w_4\varrho),$$

Hier ist $x_3^2 + Dy_3^2 = x_4^2 + Dy_4^2 = k_h$ ein Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$, es ist aber $z_3 + w_3\varrho$ nur Teiler von $m + n\varrho$ und nicht von $r + s\varrho$ und ebenso ist $z_4 + w_4\varrho$ nur Teiler von $r + s\varrho$.

Schreiben wir die Gleichung

$$x^2 + Dy^2 = k_h$$

in der Form

$$x^2 = k_h - Dy^2,$$

so folgt, daß alle Lösungspaare derselben durch eine endliche Anzahl von Proben gefunden werden können, nämlich in dem wir für y alle ganzen positiven Zahlen von 0 bis zur größten ganzen Zahl in $\sqrt{\frac{k_h}{D}}$ versuchsweise einsetzen. Für alle größeren Werte von y wird x^2 negativ, was für reelles ganzzahliges x unmöglich ist. Die Anzahl der Lösungspaare ist also endlich, weil die Anzahl der notwendigen Proben endlich ist. Diese Anzahl läßt sich beschränken, was sehr wichtig ist, wenn diese Anzahl sehr groß wird. Wir werden das später in einem besonderen Abschnitt zeigen.

Einem solchen Lösungspaar x, y entsprechen 4 Zahlen: $x + y\varrho$, $-x - y\varrho$, $x - y\varrho$, $-x + y\varrho$, welche wir paarweise als nicht wesentlich verschieden betrachten können. Wir brauchen nur $x + y\varrho$ und $x - y\varrho$ beizubehalten. Entsprechend brauchen wir nur $\frac{x+y\varrho}{2}$ und $\frac{x-y\varrho}{2}$ beizubehalten, wenn die Zahlen x, y ein Lösungspaar der Gleichung $x^2 + Dy^2 = 4k_h$ sind. Alle diese Zahlen werden wir auch Lösungen nennen.

Dem größten gemeinschaftlichen Teiler der Zahlen $m + n\varrho$ und $r + s\varrho$ entspricht auch die größte Zahl k_h welche ein solches Lösungspaar x, y einer der Gleichungen $x^2 + Dy^2 = k_h$ oder $x^2 + Dy^2 = 4k_h$ gestattet, für welches gleichzeitig die Quotienten $\frac{m+n\varrho}{z+w\varrho}$ und $\frac{r+s\varrho}{z+w\varrho}$ resp. $\frac{m+n\varrho}{z-w\varrho}$ und $\frac{r+s\varrho}{z-w\varrho}$ ganz sind. Es ist auch wie bisher $z = x$ oder $\frac{x}{2}$, $w = y$ oder $\frac{y}{2}$. Daß k_h die größte Zahl dieser Art sein muß, folgt aus dem Satz 1, § 2 und aus dem Begriff „Größter gemeinschaftlicher Teiler" für quadratische imaginäre Zahlen und wir brauchen die Zahlen k_h der Reihe nach auszuprobieren.

Die Gleichung $x^2 + Dy^2 = 4k_h$ ist in gewissem Sinne eine Erweiterung der Gleichung $x^2 + Dy^2 = k_h$, denn ist x, y ein Lösungspaar der Gleichung $x^2 + Dy^2 = k_h$, so ist $2x, 2y$ ein Lösungspaar der Gleichung $x^2 + Dy^2 = 4k_h$. Der Lösung $x + y\varrho$ der ersten Gleichung entspricht $\frac{2x+2y\varrho}{2} = x + y\varrho$ als Lösung der zweiten. Um die doppelte Bestimmung dieser Lösungen zu vermeiden, fingen wir direkt mit der Gleichung

$$x^2 + Dy^2 = 4k_h$$

an und untersuchen nur die Lösungen dieser Gleichung.

Weil also jeder gemeinschaftliche Teiler eine Lösung einer der Gleichungen $x^2 + Dy^2 = 4k_h$ ist, aber nicht umgekehrt, so ist das Verfahren selbst das folgende.

Wir fingen mit dem größten gemeinschaftlichen Teiler von $m^2 + Dn^2$ und $r^2 + Ds^2$ an, den wir in der Reihe (4) mit k bezeichneten, und bestimmen alle ganzen Lösungspaare der Gleichung

$$x^2 + Dy^2 = 4k.$$

Diese Lösungspaare seien die Zahlen

$$x_{01}, y_{01}; x_{02}, y_{02}; \ldots; x_{0g}, y_{0g}; \ldots; x_{0l}, y_{0l}.$$

Wir müssen diese alle bestimmen; jedes Lösungspaar gibt Anlaß zu zwei Zahlen $\frac{x_{0g} \pm y_{0g}\varrho}{2} = z_{0g} + w_{0g}\varrho$ und mit allen diesen müssen wir die Divisionen versuchen. Stoßen wir bei diesen Divisionen auf eine Zahl $z_{0g} + w_{0g}\varrho$, die nach früherem als gemeinschaftlicher Teiler sich ergibt, so ist das der größte und wir brauchen es mit den weiteren Lösungen nicht mehr zu versuchen, denn sie ist dann die einzige dieser Art. Die entgegengesetzte Annahme würde uns nämlich zu einem Verstoß gegen die Eindeutigkeit der Zerlegung von $m + n\varrho$ und $r + s\varrho$ in unzerlegbare Faktoren führen, denn seien etwa $z_{0i} + w_{0i}\varrho$ und $z_{0j} + w_{0j}\varrho$ die zwei Zahlen, welche Lösungen von $x^2 + Dy^2 = 4k_h$ sind und unsere Divisionen befriedigen, dann gelten die Beziehungen:

$$m + n\varrho = (m_1 + n_1\varrho)(z_{0i} + w_{0i}\varrho)$$

und

$$r + s\varrho = (r_1 + s_1\varrho)(z_{0i} + w_{0i}\varrho)$$

auch

$$m + n\varrho = (m_2 + n_2\varrho)(z_{0j} + w_{0j}\varrho)$$

und

$$r + s\varrho = (r_2 + s_2\varrho)(z_{0j} + w_{0j}\varrho).$$

Kommen in $m_1 + n_1\varrho$ und $r_1 + s_1\varrho$ oder in $m_2 + n_2\varrho$ und $r_2\varrho + s_2\varrho$ noch gemeinschaftliche Faktoren vor, so können wir sie zum anderen Faktor hinüber geworfen denken und finden somit einen gemeinsamen Teiler, dessen Norm größer als k ist, was unmöglich ist. Die Zahlen $z_{0,i} + w_{0i}\varrho$ und $z_{0j} + w_{0j}\varrho$ können nicht wesentlich verschieden sein, sonst können sie sich nur durch einen Faktor unterscheiden. Bei dieser Annahme können aber nicht $m_1 + n_1\varrho$ mit $r_1 + s_1\varrho$ und $m_2 + n_2\varrho$ mit $r_2 + s_2\varrho$ zugleich teilerfremd sein. Wenn aber auch diese Faktoren keinen gemeinschaftlichen Teiler enthalten, so wäre damit eine zweideutige Zerlegung von $m + n\varrho$ und $r + s\varrho$ in ihre unzerlegbaren Faktoren gegeben.

Wir brauchen bei allen diesen Divisionen nur zunächst ein Glied des Quotienten zu bestimmen, das zweite aber nur dann, wenn das erste eine ganze Zahl oder die Hälfte einer ganzen Zahl ist, sonst ist der ganze Quotient gewiß keine ganze Zahl.

Wenn wir zu einer Zahl $z_{0i} + w_{0i}\varrho$ gekommen sind, — zu einer solchen Zahl müssen wir schließlich kommen, was aus der Entstehung dieser Zahlen folgt, — welche ein Teiler von $m + n\varrho$ ist, dann brauchen wir nur noch zu probieren, ob $z_{0g} + w_{0g}\varrho$ auch ein Teiler von $r + s\varrho$ ist. Wenn das der Fall ist, dann ist $z_{0g} + w_{0g}\varrho$ der gesuchte größte gemeinschaftliche Teiler, wenn nicht, dann müssen unter allen diesen Zahlen zwei sein, sagen wir $z_{0e} + w_{0e}\varrho$ und $z_{0f} + w_{0f}\varrho$, von welchen die eine Teiler von $m + n\varrho$, die andere von $r + s\varrho$ ist, was auch aus der Entstehung dieser Zahlen folgt, d. h.

$$m + n\varrho = (m_{0e} + n_{0e}\varrho)(z_{0e} + w_{0e}\varrho)$$
$$r + s\varrho = (r_{0f} + s_{0f}\varrho)(z_{0f} + w_{0f}\varrho).$$

Die Zahlen $m_{0e} + n_{0e}\varrho$ und $r_{0f} + s_{0f}\varrho$ sind teilerfremd, demnach ist der größte gemeinschaftliche Teiler von $m + n\varrho$ und $r + s\varrho$ auch der größte gemeinschaftliche Teiler von $z_{0e} + w_{0e}\varrho$ und $z_{0f} + w_{0f}\varrho$, in Zeichen:

$$G(m + n\varrho, r + s\varrho) = G(z_{0e} + w_{0e}\varrho, z_{0f} + w_{0f}\varrho)$$

also ist

$$z_{0e} + w_{0e}\varrho = (m_{02} + n_{02}\varrho)(z + w\varrho)$$
$$z_{0f} + w_{0f}\varrho = (r_{02} + s_{02}\varrho)(z + w\varrho)$$

also

$$N(z_{0e} + w_{0e}\varrho) = k_h = N(m_{02} + n_{02}\varrho)\, N(z + w\varrho)$$
$$N(z_{0f} + w_{0f}\varrho) = k_h = N(r_{02} + s_{02}\varrho)\, N(z + w\varrho)$$

d. h. $z^2 + Dw^2$ ist ein Teiler von k, und weil $z + w\varrho$ der größte gemeinschaftliche Teiler dieser Zahlen ist, so ist für $z^2 + Dw^2$ die auf k folgende Zahl der Reihe (4), die wir mit k_1 bezeichnet haben zu setzen, und wir suchen die Zahlen z, w aus den Lösungspaaren

$$x_{11}, y_{11};\ x_{12}, y_{12};\ \ldots;\ x_{1t}, y_{1t}$$

der Gleichung

$$x^2 + Dy^2 = 4k_1.$$

So verfahren wir weiter. Da aber die Zahlen k_h immer kleiner werden, so kommen wir entweder zu einer Gleichung

$$x^2 + Dy^2 = 4k_h,$$

welche eine brauchbare Lösung $z + w\varrho$ liefert, oder schließlich zu der Gleichung

$$x^2 + Dy^2 = 4,$$

welche die Einheiten liefert, und dies besagt, daß $m + n\varrho$ und $r + s\varrho$ teilerfremd sind.

Wir können dieses Verfahren in folgender Weise schematisieren.

Wir bestimmen

$$G(m^2 + Dn^2, r^2 + Ds^2) = k,$$

es seien

$$k, k_1, k_2, \ldots, k_{t-1}, 1$$

alle Teiler von k.

Wir bestimmen alle ganzzahligen Lösungspaare der Gleichung

$$x^2 + Dy^2 = 4k.$$

Sie seien

$$x_{01}, y_{01};\ x_{02}, y_{02};\ \ldots;\ x_{0l}, y_{0l}.$$

Wir dividieren $m + n\varrho$ durch alle wesentlich verschiedenen Zahlen der Reihe:

$$z_{01} \pm w_{01}\varrho,\ z_{02} \pm w_{02}\varrho,\ \ldots,\ z_{0e} \pm w_{0e}\varrho,$$

wo

$$z_{01} = \frac{x_{01}}{2},\ w_{01} = \frac{y_{01}}{2},\ \ldots$$

bis wir zu einem ganzen Quotienten $\frac{m + n\varrho}{z_{0g} + w_{0g}\varrho}$ oder $\frac{m + n\varrho}{z_{0g} - w_{00}}$ kommen. Ist dann auch $\frac{r + s\varrho}{z_{0g} + w_{0g}\varrho}$ beziehungsweise $\frac{r + s\varrho}{z_{0g} - w_{0g}\varrho}$ ganz, so ist

$$G(m + n\varrho, r + s\varrho) = z_{0g} + w_{0g}\varrho \text{ oder } z_{0g} - w_{0g}\varrho.$$

Ist das mit keiner Zahl $z_{0g} \pm w_{0g}$ erreicht, dann lösen wir die Gleichung

$$x^2 + Dy^2 = 4k_1$$

auf. Die Lösungspaare heißen

$$x_{11}, y_{11}; x_{12}, y_{12}; \ldots; x_{1t}, y_{1t}.$$

Wir verfahren mit den Zahlen $z_{11} \pm w_{11}\varrho$, $z_{12} \pm w_{12}\varrho$, ... genau so wie mit den Zahlen $z_{01} \pm w_{01}\varrho$, $z_{02} \pm w_{02}\varrho$, ... und so lange bis wir entweder zu einer Gleichung

$$x^2 + Dy^2 = 4k_h$$

kommen, bei der $m + n\varrho$ und $r + s\varrho$ durch eine Zahl $z_{hg} \pm w_{hg}\varrho$ dividiert, ganze Quotienten ergeben, dann ist diese Zahl $= G(m + n\varrho, r + s\varrho)$ oder bis wir zur Gleichung kommen

$$x^2 + Dy^2 = 4$$

und dann ist $m + n\varrho$ mit $r + s\varrho$ teilerfremd.

Dieses Verfahren ist immer anwendbar, und der größte gemeinschaftliche Teiler wird durch eine endliche Anzahl von Proben gefunden.

Die Anzahl der nötigen Proben kann unter Umständen sehr groß werden, doch bleibt sie immer endlich. Diese Anzahl kann auch bedeutend verkleinert werden dadurch, daß wir auf die gegebenen Zahlen $m + n\varrho$ und $r + s\varrho$ zunächst den Euklidischen Algorithmus anwenden. Eigentlich führt auch dieser, solange er anwendbar ist, zum Ziel nur durch Probieren und mittels einer endlichen Probeanzahl, denn jede Division bedeutet eine Probe, ob die kleinere Zahl ein Teiler der größeren ist und, wenn das nicht der Fall ist, ein Übergang zum Probieren von neuen Zahlen. Die Probeanzahl oder die Anzahl der nach einander folgenden Divisionen kann unter Umständen auch ziemlich groß werden.

Beim Versagen des Euklidischen Algorithmus kann man den hier angegebenen Weg, der nie versagt, einschlagen. In vielen Fällen kommt man dadurch leichter zum Ziel als mittels des Euklidischen Algorithmus auch wenn der letzte anwendbar ist.

In dieser Weise kann man den größten gemeinschaftlichen Teiler auch für eine beliebige Anzahl gegebener Zahlen durch eine endliche Anzahl von Operationen immer bestimmen.

Beispiel:

Es ist $G\left(18 + 23\varrho, \frac{45 - 79\varrho}{2}\right)$ zu suchen, $\varrho = \sqrt{-3}$

$$18^2 + 3 \cdot 23^2 = 1911, \quad \frac{45^2 + 3 \cdot 79^2}{4} = 5187$$

$$G(5187, 1911) = 273.$$

Die Teiler von 273 sind

$$273, 91, 39, 21, 13, 7, 3, 1.$$

Die erste Gleichung, welche wir aufzulösen haben, lautet

$$x^2 + 3y^2 = 1092; \quad \left[\sqrt{\frac{1092}{3}}\right] = \left[\sqrt{364}\right] = 19,$$

also 20 Proben. Die Lösungspaare sind

$$y = \pm 1, \quad \pm 8, \quad \pm 11, \pm 16, \pm 17, \pm 19$$
$$x = \pm 33, \pm 30, \pm 27, \pm 18, \pm 15, \pm 3,$$

also haben wir die Zahl $18 + 23\varrho$ durch alle wesentlich verschiedenen Zahlen der Reihe

$$\frac{33 \pm \varrho}{2},\ 15 \pm 4\varrho,\ \frac{27 \pm 11\varrho}{2},\ 9 \pm 8\varrho,\ \frac{15 \pm 17\varrho}{2},\ \frac{3 \pm 19\varrho}{2}$$

zu dividieren.

Wir werden jetzt die nicht wesentlich verschiedenen Lösungen, welche sich durch eine Einheit $\frac{1+\varrho}{2}$ oder $\frac{1-\varrho}{2}$ unterscheiden, bestimmen.

$$\frac{33+\varrho}{2} \cdot \frac{1+\varrho}{2} = \frac{15+17\varrho}{2}; \quad \frac{33+\varrho}{2} \cdot \frac{1-\varrho}{2} = 9 - 8\varrho.$$

Die Lösungen

$$\frac{33+\varrho}{2},\ \frac{15+17\varrho}{2},\ 9 - 8\varrho$$

sind nicht wesentlich verschieden und infolgedessen sind

$$\frac{33-\varrho}{2},\ \frac{15-17\varrho}{2},\ 9 + 8\varrho$$

auch nicht wesentlich verschieden.

$$(15 + 4\varrho) \cdot \frac{1+\varrho}{2} = \frac{3+19\varrho}{2},\ (15 + 4\varrho)\frac{1-\varrho}{2} = \frac{27-11\varrho}{2}$$

also sind

$$15 + 4\varrho,\ \frac{3+19\varrho}{2},\ \frac{27-11\varrho}{2},\ \text{folglich auch}\ 15 - 4\varrho,\ \frac{3-19\varrho}{2},\ \frac{27+11\varrho}{2}$$

nicht wesentlich verschieden. Jetzt dividieren wir die gegebene Zahl $18 + 23\varrho$ der Reihe nach durch $15 \pm 4\varrho$, $9 \pm 8\varrho$

$$\frac{18+23\varrho}{15+4\varrho} = \frac{546}{273} + \frac{273}{273}\varrho = 2 + \varrho,$$

also ganz aber

$$\frac{45-79\varrho}{2(15+4\varrho)} = \frac{546}{948} + \ldots = \frac{91}{158} + \ldots$$

also nicht ganz. Die Zahlen $15 - 4\varrho$ und $9 \pm 8\varrho$ brauchen nicht ausprobiert zu werden, weil $18 + 23\varrho$ durch $15 + 4\varrho$ dividierbar ist, demnach kann sie, wie wir gesehen haben, durch keine von diesen drei Zahlen dividierbar sein. Wir müssen jetzt zur nächsten Gleichung übergehen.

$$x^2 + 3y^2 = 364; \quad \left[\sqrt{\frac{364}{3}}\right] = [\sqrt{121}] = 11$$

also zwölf Proben. Die Lösungspaare sind

$$y = \pm 1, \quad \pm 5, \quad \pm 6, \quad \pm 9, \quad \pm 10, \pm 11,$$
$$x = \pm 19, \pm 17, \pm 16, \pm 11, \pm 8, \quad \pm 1.$$

Die Lösungen sind also:

$$\frac{19 \pm \varrho}{2},\ \frac{17 \pm 5\varrho}{2},\ 8 \pm 3\varrho,\ \frac{11 \pm 9\varrho}{2},\ 4 \pm 5\varrho,\ \frac{1 \pm 11\varrho}{2}.$$

Die nicht wesentlich verschiedenen Lösungen sind

$$\frac{19+\varrho}{2},\ 4+5\varrho \text{ und } \frac{11-9\varrho}{2};\ \frac{19-\varrho}{2},\ 4-5\varrho \text{ und } \frac{11+9\varrho}{2}$$

$$\frac{17+5\varrho}{2},\ \frac{1+11\varrho}{2} \text{ und } 8-3\varrho;\ \frac{17-5\varrho}{2},\ \frac{1-11\varrho}{2} \text{ und } 8+3\varrho.$$

Wir brauchen also die gegebene Zahl $18 + 23\varrho$ der Reihe nach durch vier Zahlen zu dividieren. Das können die Zahlen $4 \pm 5\varrho$ und $8 \pm 3\varrho$ sein

$\frac{18+23\varrho}{4+5\varrho} = \frac{417}{91} + \ldots$ also nicht ganz $\frac{18+23\varrho}{4-5\varrho} = \frac{-273}{91} + \frac{182}{91}\varrho = -3+2\varrho$

also ganz

$$\frac{45-79\varrho}{2(4-5\varrho)} = \frac{2730}{364} + \frac{-182}{364}\varrho = \frac{15-\varrho}{2} \text{ also auch ganz.}$$

Demnach ist

$$G\left(18+23\varrho,\ \frac{45-79\varrho}{2}\right) = 4-5\varrho.$$

In allen anderen Körpern ist dieses Verfahren einfacher und führt in vielen Fällen am schnellsten zum Ziel.

Beispiel: Es ist $G\left(\frac{283-151\varrho}{2},\ \frac{91-15\varrho}{2}\right)$ zu bestimmen $\varrho = \sqrt{-7}$

$$N\left(\frac{283-151\varrho}{2}\right) = 59924,\ N\left(\frac{91-15\varrho}{2}\right) = 2464$$

$$G(59924,\ 2464) = 4.$$

Die Teiler von 4 sind $\pm 4, \pm 2, \pm 1$;

$$x^2 + 7y^2 = 16,\ \left[\sqrt{\frac{16}{7}}\right] = [\sqrt{2}] = 1$$

also zwei Proben. Das einzige Lösungspaar ist $y = \pm 1$, $x = \pm 3$. Die Lösungen sind $\frac{3 \pm \varrho}{2}$

$$\frac{2(283-151\varrho)}{2(3+\varrho)} = 13 + 46\varrho \text{ also ganz}$$

$$\frac{(91-15\varrho)}{(3+\varrho)} = \frac{21-17\varrho}{2} \text{ also ganz.}$$

Dementsprechend ist

$$G\left(\frac{283-151\sqrt{-7}}{2},\ \frac{91-15\sqrt{-7}}{2}\right) = \frac{3+\sqrt{-7}}{2}$$

§ 5. Die Zerlegung von eindeutig zerlegbaren quadratischen imaginären Zahlen in unzerlegbare Faktoren.

Die quadratische Gleichung

$$x^2 + Dy^2 = 4k_h$$

und die Betrachtung der Normen der zu untersuchenden Zahlen, die uns eben zur Auffindung des größten gemeinschaftlichen Teilers dieser Zahlen verholfen haben, wird uns hier die Zerlegung von $a + b\varrho$ oder $\frac{a+b\varrho}{2}$, wo $\varrho = \sqrt{-D}$ und D eine der Zahlen

$$1, 2, 3, 7, 11, 19, 27, 43, 67, 163$$

ist, in unzerlegbare Faktoren ergeben.

Enthält die Zahl $a + b\varrho$ oder $\frac{a+b\varrho}{2}$ einen ganzen rationalen Faktor, so läßt sich dieser leicht finden mittels des Euklidischen Algorithmus auf a und b angewandt. Die Zahl $a + b\varrho$ oder $\frac{a+b\varrho}{2}$ kann auch eine rationale Zahl sein. In diesen beiden Fällen haben wir die Aufgabe, eine gewisse rationale Zahl in unzerlegbare Faktoren zu zerlegen; da diese Aufgabe sich einfacher behandeln läßt wie die allgemeine, so werden wir diese zuerst behandeln.

Wir zerlegen die gegebene Zahl in rationale Primfaktoren und dann ist die Aufgabe auf die Zerlegung in Primfaktoren einer rationalen Primzahl reduziert. Dazu werden wir $a + b\varrho$ oder $\frac{a+b\varrho}{2}$ durch $m + n\varrho$ bezeichnen und den folgenden Satz beweisen.

Satz 1: *Ist $m + n\varrho$ eine unzerlegbare Zahl, so ist es $m - n\varrho$ auch.*

In der Tat, wäre

$$\frac{m-n\varrho}{r+s\varrho} = \frac{mr-Dns}{r^2+Ds^2} + \frac{ms-nr}{r^2+Ds^2}\varrho = u + v\varrho$$

ganz, so muß auch

$$\frac{m+n\varrho}{r-s\varrho} = \frac{mr-Dns}{r^2+Ds^2} + \frac{-ms+nr}{r^2+Ds^2}\varrho = u - v\varrho$$

ganz sein; da aber $m + n\varrho$ unzerlegbar ist, so kann sie keinen Teiler $r - s\varrho$ enthalten; also muß auch $m - n\varrho$ eine unzerlegbare Zahl sein, q. e. d.

Es sei jetzt p eine rationale Primzahl. Die Zahl p kann nicht einen ganzen rationalen Faktor r, welcher von p verschieden ist, enthalten. Enthält p einen Faktor der Form $s\varrho$, so ist $s \neq p$. Es sei $\frac{p}{s\varrho} = z + w\varrho$, also wird auch $p = -Dsw + zs\varrho$ sein, d. h. $zs = 0$ also $z = 0$, weil s von 0 verschieden ist, und $-Dsw = p$, was nur möglich ist, wenn entweder $D = \pm 1$, $sw = \pm p$ oder $D = \pm p$, $sw = \mp 1$ und dann ist in beiden Fällen der mögliche Faktor dieser Form $= \pm \varrho$.

Satz 2: *Die Zahl ϱ ist in jedem ihr entsprechenden Körper eine unzerlegbare Zahl.*

In der Tat, wäre $r + s\varrho$ eine unzerlegbare Zahl, welche in ϱ aufgeht, d. h. wäre

$$\frac{\varrho}{r + s\varrho} = \frac{Ds}{r^2 + Ds^2} + \frac{r}{r^2 + Ds^2}\varrho = u + v\varrho$$

ganz, so wäre, entsprechend

$$\frac{\varrho}{r - s\varrho} = \frac{-Ds}{r^2 + Ds^2} + \frac{r}{r^2 + Ds^2}\varrho = -u + v\varrho$$

auch ganz. Da aber $r + s\varrho$ unzerlegbar ist, so ist es $r - s\varrho$ auch (Satz 1). Folglich wäre ϱ durch das Produkt dieser Zahlen teilbar, d. h. es muß ϱ durch eine ganze rationale Zahl $r^2 + Ds^2$ teilbar sein, was unmöglich ist.

Satz 3: *Hat die Zahl p einen unzerlegbaren Teiler $r + s\varrho$, wo r und s von 0 verschieden sind, so ist*

$$r^2 + Ds^2 = p.$$

Beweis: Ist

$$\frac{p}{r + s\varrho} = \frac{pr}{r^2 + Ds^2} + \frac{-ps}{r^2 + Ds^2}\varrho = u - v\varrho$$

ganz, so ist entsprechend auch

$$\frac{p}{r - s\varrho} = \frac{pr}{r^2 + Ds^2} + \frac{ps}{r^2 + Ds^2} = u + v\varrho$$

ganz.

Ist aber $r + s\varrho$ eine unzerlegbare Zahl, so ist es, wie bewiesen (Satz 1), $r - s\varrho$ auch, also ist p durch das Produkt

$$(r + s\varrho)(r - s\varrho) = r^2 + Ds^2$$

teilbar; da aber p eine rationale Primzahl und $r^2 + Ds^2$ eine ganze rationale Zahl ist (Satz 3, § 2), so ist es nur möglich, wenn

$$r^2 + Ds^2 = p$$

ist, q. e. d.

Satz 4: *Umgekehrt. Erfüllen r und s die Gleichung $z^2 + Dw^2 = p$ und sind r und s ganze Zahlen oder die Hälften von solchen, so ist $r + s\varrho$ eine unzerlegbare Zahl.*

In der Tat, wäre $r_1 + s_1\varrho$ eine unzerlegbare Zahl, welche in $r + s\varrho$ aufgeht, so geht sie auch in p auf, weil $r + s\varrho$ ein Teiler von p ist. Da-

mit ist aber auch $r_1 - s_1\varrho$ ein unzerlegbarer Teiler von p, folglich wäre dann $r_1^2 + Ds_1^2$ ein Teiler von p, also $= p$, dann muß aber $r_1^2 + Ds_1^2$ durch $r + s\varrho$ dividierbar sein, weil aber $r_1^2 + Ds_1^2$ aus zwei unzerlegbaren Faktoren $r_1 + s_1\varrho$ und $r_1 - s_1\varrho$ besteht, so kann $r + s\varrho$ nur gleich $r_1 + s_1\varrho$ oder $= r_1 - s_1\varrho$ sein.

Weil hier $r = \alpha$ oder $\frac{\alpha}{2}$ und $s = \beta$ oder $\frac{\beta}{2}$ sind, so ist α, β ein Lösungspaar einer der Gleichungen

$$x^2 + Dy^2 = p \text{ oder } x^2 + Dy^2 = 4p$$

und aus dem zuletzt bewiesenen Satz folgt unmittelbar

Satz 5: *Wenn p in Faktoren zerlegbar ist, so sind das zwei konjugierte unzerlegbare Zahlen.*

Satz 6: *Wenn die Faktoren von p sich nicht wesentlich unterscheiden, so ist p ein Quadrat einer unzerlegbaren Zahl.*

Satz 7: *Wenn $x^2 + Dy^2 = p$ ein Lösungspaar α, β hat, so kann $x^2 + Dy^2 = 4p$ nur das Lösungspaar $2\alpha, 2\beta$ haben.*

Satz 8: *Wenn $x^2 + Dy^2 = 4p$ ein Lösungspaar hat, so ist es das einzige.*

Der letzte Satz ist das Eulersche Kennzeichen für Primzahlen.

Ist $x^2 + Dy^2 = p$ oder $= 4p$, so ist p quadratischer Rest der Zahl D. Ist diese Zahl ein Nichtrest, so kann auch nicht $x^2 + Dy^2 = p$ oder $= 4p$ sein, d. h. p ist auch in dem Körper $R(\varrho)$ eine unzerlegbare Zahl. Das kann auch als Kennzeichen der Zerlegbarkeit der Zahl p benutzt werden. Diese Gleichungen sagen aber mehr aus, denn die Feststellung, ob p quadratischer Rest von D ist oder nicht, ist nicht einfacher als die Auflösung einer dieser Gleichungen, wodurch nicht nur die Zerlegbarkeit bewiesen, sondern auch die Zerlegung selbst angegeben wird.

Die Zahlen a und b in der Zahl $a + b\varrho$ oder $\frac{a + b\varrho}{2}$ können wir jetzt im rat. Körper als relativprim betrachten, und es ist nun noch die so beschaffene Zahl $m + n\varrho$ in unzerlegbare Faktoren zu zerlegen.

Nehmen wir an

$$(m + n\varrho) = (z_1 + w_1\varrho)(z_2 + w_2\varrho) \dots (z_h + w_h\varrho),$$

wo

$$z_1 + w_1\varrho, \quad z_2 + w_2\varrho, \dots, z_h + w_h\varrho$$

ganze unzerlegbare Zahlen sind. Dann ist auch

$$N(m + n\varrho) = N(z_1 + w_1\varrho)N(z_2 + w_2\varrho) \dots N(z_h + w_h\varrho),$$

wo

$$N(m + n\varrho), \quad N(z_1 + w_1\varrho), \dots, N(z_h + w_h\varrho)$$

ganze rationale Zahlen sind (Satz 3, § 2). $N(m + n\varrho)$ zerlegen wir in

rationale Primfaktoren, bestimmen dann alle Faktoren dieser Zahl und ordnen sie nach steigender Größe.

(1) $$1, l_1, l_2, \ldots, l_t,$$

wo l_t die $N(m + n\varrho)$ selbst ist.

Die Norm jedes unzerlegbaren Faktors von $m + n\varrho$ ist also Teiler von $N(m + n\varrho)$, also unter den Zahlen l_h enthalten. Bezeichnen wir wieder $z_i + w_i\varrho = x_i + y_i\varrho$ oder $\frac{x_i + y_i\varrho}{2}$, wo x_i, y_i ganze Zahlen sind, so sind demnach x_i, y_i unter den ganzzahligen Lösungen der Gleichung $x^2 + Dy^2 = l_h$ oder $x^2 + Dy^2 = 4l_h$ zu suchen. Umgekehrt braucht nicht jedes Lösungspaar dieser Gleichung Teiler von $m + n\varrho$ zu liefern, darüber kann uns nur die Ausführung der Division Auskunft geben.

Weiterhin entspricht dem kleinsten l_h, dem ein passendes Lösungspaar entspricht, sicherlich eine unzerlegbare Zahl und weil, wie wir gezeigt haben, die Gleichung $x^2 + Dy^2 = 4l_h$ auch alle Lösungen der Gleichung $x^2 + Dy^2 = l_h$ liefert, so fangen wir infolgedessen hier mit der Gleichung

(2) $$x^2 + Dy^2 = 4l_1,$$

wo l_1 der kleinste Divisor von l ist, an und untersuchen nacheinander in der schon bekannten Weise alle solchen Gleichungen für steigende l, bis wir zu einer Zahl l_h kommen, für welche

$$x^2 + Dg^2 = 4l_h$$

Lösungen hat.

Jedes Lösungspaar dieser Gleichung bietet uns zwei konjugierte Zahlen $\frac{x_{h\lambda} \pm y_{h\lambda}\varrho}{2} = z_{h\lambda} + w_{h\lambda}\varrho$. In $R(i)$ und $R(\sqrt{-3})$ brauchen wir nun noch aus den gefundenen Lösungen alle nicht wesentlich verschiedenen auszusuchen und diese durch Division auszuprobieren. Ist eine der Zahlen $\frac{m + n\varrho}{z + w\varrho}$ oder $\frac{m + n\varrho}{z - w\varrho}$ ganz, so ist die entsprechende Zahl $z + w\varrho$ oder $z - w\varrho$ ein unzerlegbarer Faktor von $m + n\varrho$, weil l_h die erste Zahl der Reihe (1) ist, welche passende Lösungen der Gleichung $x^2 + Dy^2 = 4l_h$ zuläßt.

Nur eine von diesen Zahlen kann aber ein Teiler von $m + n\varrho$ sein, und nur ein Lösungspaar $x_{h\lambda}, y_{h\lambda}$ kann einen Teiler liefern, weil sonst entweder $m + n\varrho$ durch eine rationale Zahl $N(x_h + y_h\varrho)$ dividierbar sein muß, m und n sind aber $= a$ und b oder $\frac{a}{2}$ und $\frac{b}{2}$ und die Zahlen a und b sind relativ prim vorausgesetzt, oder weil sonst die Zerlegung in wesentlich verschiedene Faktoren nicht mehr eindeutig ist. Die Zahl $z_{h\lambda} + w_{h\lambda}\varrho$ ist $m + n\varrho$ selbst, wenn $l_h = l_t$ ist, d. h. in diesem Fall ist $m + n\varrho$ eine unzerlegbare Zahl.

Sobald wir zu einem unzerlegbaren Teiler gekommen sind, dann haben wir die ganze Überlegung auf die Zahl $\frac{m+n\varrho}{z_{h\lambda}+w_{h\lambda}} = m_h + n_h\varrho$ oder $\frac{m+n\varrho}{z_{h\lambda}-w_{h\lambda}\varrho} = m_{h'} + n_{h'}\varrho$ wieder anzuwenden. Hier ist $m_h^2 + Dn_h^2$ oder $m_{h'}^2 + D_{h'}^2 = \frac{l_t}{l_h}$ und die entsprechende Teilerreihe besteht aus der früheren (1), mit Ausnahme von l_h und allen Zahlen, welche l_h enthalten. Die Zahlen l_h sind schon ausprobiert und können auch ausgelassen werden. Die schon gefundenen Teiler müssen wir aber durch Division weiter ausprobieren, weil in $N(m+n\varrho)$ Potenzen einer Primzahl vorkommen können.

Dies Verfahren haben wir so lange zu wiederholen, bis wir entweder zu einer passenden Zahl l_h kommen oder die Reihe (1) ganz erschöpfen.

Beispiel: Es soll die Zahl $\frac{429+129\varrho}{2}$, wo $\varrho = \sqrt{-11}$ in unzerlegbare Faktoren zerlegt werden,

$$G(429, 129) = 3,$$

also ist

$$\frac{429+129\varrho}{2} = \frac{3(143+43\varrho)}{2};$$

(A) $$x^2 + 11y^2 = 12$$

hat das Lösungspaar $x = \pm 1$, $y = \pm 1$, also sind $\frac{1+\varrho}{2}$ und $\frac{1-\varrho}{2}$ die unzerlegbaren Teiler von 3.

$$N\left(\frac{143+43\varrho}{2}\right) = \frac{143^2+11\cdot 43^2}{4} = 10197 = 3^2\cdot 11\cdot 103.$$

Die Reihe der Faktoren von 10197 ist

1, 3, 9, 11, 33, 99, 103, 309, 927, 1133, 3399, 10197.

Die Zahl 3 ist schon in der Gleichung (A) ausprobiert, wir brauchen die Zahlen $\frac{1+\varrho}{2}$ und $\frac{1-\varrho}{2}$ noch als Teiler auszuprobieren

$$\frac{2(143+43\varrho)}{2(1\pm\varrho)} = \frac{143\pm 11\cdot 43}{12} + \cdots = \frac{616}{12} + \cdots \text{ oder } \frac{-330}{12} + \frac{186}{12}\varrho = \frac{-55+31\varrho}{2}$$

also ganz,

$$\frac{2(-55+31\varrho)}{2(1-\varrho)} = -33 - 2\varrho$$

also ganz,

$$\frac{2(-33-2\varrho)}{2(1-\varrho)} = \frac{-9}{12} + \cdots$$

also nicht ganz. Dem entsprechend ist $\left(\frac{1-\varrho}{2}\right)^2$ noch eine Zahl der gesuchten Zerlegung.

Die Reihe der Teiler, welche jetzt noch nötig ist auszuprobieren, ist

11, 103, 1133.

Die Zahl 11 hat in $R(\sqrt{-11})$ einen Teiler $\sqrt{-11}$, welchen wir ausprobieren müssen. Demnach brauchen wir die Gleichung

$$x^2 + 11y^2 = 44$$

nicht zu untersuchen, denn $\sqrt{-11}$ wird ihre Lösung sein.

$$\frac{33+2\varrho}{\varrho} = \frac{22}{11} - \frac{33}{11}\varrho = 2 - 3\varrho$$

also ganz, und folglich ist ϱ ein Teiler.

Es bleibt noch $2 - 3\varrho$ in Faktoren zu zerlegen; da aber die Normen der möglichen Faktoren von $2 - 3\varrho$ in der Reihe der Zahlen, welche wir noch ausprobieren müssen, enthalten sind und diese Reihe aus der einen Primzahl 103 besteht, so ist $2 - 3\varrho$ eine unzerlegbare Zahl und die vollständige Zerlegung ist:

$$\frac{429+129\sqrt{-11}}{2} = \frac{1+\sqrt{-11}}{2}\left(\frac{1-\sqrt{-11}}{2}\right)^3 \cdot \sqrt{-11} \cdot (2-3\sqrt{-11}).$$

Die Lösungspaare der Gleichung

$$x^2 + Dy^2 = 4k \quad \text{oder} \quad = 4l$$

für kleinzahlige k oder l lassen sich ganz leicht bestimmen mittels einer Tabelle der Quadratzahlen. Dies veranlaßt uns, eine solche Tabelle für alle ganzen Zahlen von 1 bis 100 auch hier anzugeben. Derartige Tabellen finden sich auch in einigen Ausgaben von Logarithmentafeln.

Tabelle der Quadratzahlen von 1 bis 100.

Num.	Quadr.	Num.	Quadr.	Num.	Quadr.	Num.	Quadr.
1	1	26	676	51	2601	76	5776
2	4	27	729	52	2704	77	5929
3	9	28	784	53	2809	78	6084
4	16	29	841	54	2916	79	6241
5	25	30	900	55	3025	80	6400
6	36	31	961	56	3136	81	6561
7	49	32	1024	57	3249	82	6724
8	64	33	1089	58	3364	83	6889
9	81	34	1156	59	3481	84	7056
10	100	35	1225	60	3600	85	7225
11	121	36	1296	61	3721	86	7396
12	144	37	1369	62	3844	87	7569
13	169	38	1444	63	3969	88	7744
14	196	39	1521	64	4096	89	7921
15	225	40	1600	65	4225	90	8100
16	256	41	1681	66	4356	91	8281
17	289	42	1764	67	4489	92	8464
18	324	43	1849	68	4624	93	8649
19	361	44	1936	69	4761	94	8836
20	400	45	2025	70	4900	95	9025
21	441	46	2116	71	5041	96	9216
22	484	47	2209	72	5184	97	9409
23	529	48	2304	73	5329	98	9604
24	576	49	2401	74	5476	99	9801
25	625	50	2500	75	5625	100	10000

§ 6. Behandlung der Gleichung $x^2 + Dy^2 = k$ für große k.

Die Auflösung der Gleichung

$$x^2 + Dy^2 = k,$$

welche wir angegeben haben, wird umständlich, wenn k groß ist, denn die höchste Probeanzahl, welche durch die Zahl $\left[\sqrt{\frac{k}{D}}\right]$ bestimmt ist, wird dann auch groß. Die Wichtigkeit der Auflösung dieser Gleichung bei unserer Untersuchung veranlaßt uns hier zu zeigen[1]), in welcher Weise diese Probeanzahl verkleinert und damit diese Schwierigkeit unserer Aufgabe möglichst beseitigt werden kann.

Bezeichnen wir den Ausdruck $k - Dy^2$ mit V, so folgt daraus, daß V positiv und eine Quadratzahl sein muß, erstens, daß y nicht größer als $\left[\sqrt{\frac{k}{D}}\right]$ sein kann, und daß wir nach der vorhin angegebenen Methode alle Zahlen, welche innerhalb der Grenzen 0 und $\left[\sqrt{\frac{k}{D}}\right]$ liegen, für y substituieren sollen; zweitens, daß nur diejenige beizubehalten sind, für welche V ein Quadrat wird. Bezeichnen wir alle Zahlen in dem Intervall von 0 bis $\left[\sqrt{\frac{k}{D}}\right]$ mit ω, so lassen sich aus ω beliebig viele Zahlen, ohne sie in V auszuprobieren, in folgender Weise ausschließen.

Nehmen wir an, daß E_1 eine willkürliche ganze rationale Zahl sei. Es seien ferner $a_1, a_2, a_3, \ldots$ quadratische Nichtreste von E_1. Wir berechnen die Wurzel der Kongruenzen

$$(1) \qquad Dz \equiv k - a_1, \quad Dz \equiv k - a_2, \ldots \pmod{E_1},$$

welche $g_1, g_2, g_3 \ldots$ sein mögen und wählen aus diesen Zahlen die quadratischen Reste $\alpha_1, \alpha_2, \alpha_3, \ldots$ von E_1 aus. Sind zwischen allen diesen α keine quadratische Reste vorhanden, so probieren wir eine andere Zahl E_1.

Aus der Kongruenz

$$y^2 \equiv \alpha_1 \pmod{E_1}$$

folgt

$$Dy^2 \equiv D\alpha_1 \pmod{E_1}.$$

---

1) Vgl. Gauß „Disq. arithmeticae“ § 323. Die Gl. $x^2 + Dy^2 = k$, ist aber einfacher als die Gleichung $mx^2 + ny^2 = k$, welche Gauß behandelt. Das haben wir auszunutzen versucht.

Da aber die Lösung der Kongruenz

$$Dz \equiv k - a_\lambda \pmod{E_1}$$

α_1 ist, so ist

$$D\alpha_1 \equiv k - a_\lambda \pmod{E_1},$$

also ist auch

$$Dy^2 \equiv k - a_\lambda \pmod{E_1}$$

oder

$$k - Dy^2 \equiv a_\lambda \pmod{E_1} \text{ d. i. } V \equiv a_\lambda \pmod{E_1}.$$

Ist umgekehrt für irgend welches y

$$V \equiv a_\lambda \pmod{E_1},$$

so ist für dieses y

$$y^2 \equiv \alpha_1 \pmod{E_1},$$

ist aber $V \equiv a_\lambda \pmod{E_1}$, so kann x^2 nicht diesem V gleich sein, denn anders ist auch $x^2 \equiv a_\lambda \pmod{E_1}$, a_λ ist aber Nichtrest, also sind alle V der Form $E_1 t + a_\lambda$ auszuschließen. Dazu gehören alle y der Form $E_1 t \pm h_1$, $E_1 t \pm h_2, \ldots, E_1 t \pm h_\nu$, wo $\pm h_1, \pm h_2, \ldots, \pm h_\nu$ alle Lösungen der Kongruenz $y^2 \equiv \alpha_1 \pmod{E_1}$ sind, ausgeschlossen zu werden ohne die in V zu probieren, denn setzen wir $E_1 t \pm h_\mu$ in V ein, so ist

$$V = k - D(E_1 t \pm h_\mu)^2 \equiv k - Dy^2 \equiv a_\lambda \pmod{E_1}.$$

Betrachten wir in dieser Weise $\alpha_2, \alpha_3, \ldots$, so bestimmen wir nacheinander alle Zahlen $h_{\nu+1}, h_{\nu+2}, \ldots, h_m$ und damit sind auch alle Zahlen in ω der Form $Et \pm h_1, Et \pm h_2, \ldots, Et \pm h_m$ ausgeschlossen.

Nehmen wir eine andere Zahl E_2, so bekommen wir entsprechende $\pm h$ usw.

In dieser Weise können wir aus ω auch die Zahlen

$$E_2 t \pm h_1, \quad E_2 t \pm h_2, \ldots,$$

wo $\pm h_1, \ldots$ schon durch E_2 bestimmt sind, ausschließen. Da aber die Anzahl der Zahlen in ω endlich ist, so werden wir schließlich zu einer geringen Anzahl von Zahlen aus ω, welche wir noch in V zu probieren brauchen, kommen. Wenn in dieser Weise alle Zahlen aus ω herausfallen, so ist das ein Beweis, daß die angegebene Gleichung keine Lösungen hat.

In vielen Fällen ist bequemer nicht x sondern y zu bestimmen. Bezeichnen wir in diesem Fall den Ausdruck $\frac{k - x^2}{D}$ mit V, so muß V positiv, ganz und eine Quadratzahl sein. Die erste Bedingung erfordert, daß alle y innerhalb der Grenzen 0 und $\sqrt{k}$ liegen. Die zweite erfordert, daß, wenn die Wurzel der Kongruenz

$$z \equiv k \pmod{D}$$

den Wert δ hat, wo $\delta < D$ ist, so ist δ quadratischer Rest von D. Bezeichnen wir die Wurzel der Kongruenz

$$x^2 \equiv \delta \pmod{D}$$

mit $\pm r_1, \pm r_2, \ldots$, so müssen die Werte von y unter einer der Formen

$$Dt \pm r_1, \quad Dt \pm r_2, \ldots$$

enthalten sein und wir brauchen nur die Zahlen dieser Form, welche innerhalb der angegebenen Grenzen liegen, auszuprobieren.

Bezeichnen wir die Gesamtheit aller Zahlen zwischen 0 und $\sqrt{k}$ mit ω_1, so enthält ω_1 mehr Zahlen als ω. Bei der angegebenen Form dieser Zahlen wird aber diese Anzahl bedeutend verkleinert. Auch diese Anzahl läßt sich, wie im vorhergehenden, beliebig verkleinern.

Wir bezeichnen mit E_1 wieder eine ganze rationale Zahl. Dieselbe muß aber in diesem Fall mit D relativ prim sein. Es seien wieder a_1, $a_2, \ldots$ quadratische Nichtreste von E_1. Wir bezeichnen jetzt mit $g_1, g_2, \ldots$ die Wurzel der Kongruenzen

$$(2) \qquad z \equiv k - a_1 D, \quad z \equiv k - a_2 D, \ldots \pmod{E_1},$$

da diese Kongruenzen von den (1) verschieden sind, so sind die neuen $g_1, g_2, \ldots$ nicht unbedingt die früheren. Wir wählen aus diesen Zahlen wieder die quadratischen Reste $\alpha_1, \alpha_2, \alpha_3, \ldots$ aus. Sei

$$x^2 \equiv \alpha_1 \pmod{E_1}$$

und α_1 die Lösung der Kongruenz

$$z \equiv k - a_\lambda D \pmod{E_1},$$

so ist

$$k - a_\lambda D \equiv \alpha_1 \pmod{E_1},$$

also

$$k - a_\lambda D \equiv x^2 \pmod{E_1}$$

oder

$$k - x^2 \equiv a_\lambda D \pmod{E_1}$$

oder, weil D und E_1 relativ prim sind,

$$\frac{k - x^2}{D} \equiv a_\lambda \pmod{E_1},$$

d. h.

$$y^2 = V \equiv a_\lambda \pmod{E_1},$$

was wieder unmöglich ist, weil a_λ Nichtrest ist, also sind wieder alle V der Form $E_1 t + a_\lambda$ auszuschließen. Dazu gehören, analog wie früher, alle x der Form $E_1 t \pm h_\mu$, wo $\pm h_\mu$, eine der Lösungen der Kongruenz

$$x^2 \equiv \alpha_1 \pmod{E_1}$$

ist ausgeschlossen, denn setzen wir diesen Wert in V ein, so ist

$$V = \frac{k - (E_1 t \pm h_\mu)^2}{D} \equiv \frac{k - x^2}{D} \equiv a_\lambda \pmod{E_1}.$$

In dieser Weise probieren wir alle $\alpha_1, \alpha_2, \ldots$ aus, bestimmen alle $\pm h_1, \pm h_2, \ldots$ und schließen alle Zahlen der Form

$$E_1 t \pm h_1, \; E_1 t \pm h_2, \ldots$$

aus den Zahlen $Dt \pm r_1, \ldots$ aus, durch verschiedene E werden neue h bestimmt und wir können auch aus allen Zahlen der Form $Dt \pm r_\lambda$, welche in ω enthalten sind, die Zahlen

$$E_2 t \pm h_1,\ E_2 t \pm h_1, \ldots,\ E_3 t \pm h_1, \ldots$$

ausschließen. Dieses Verfahren wiederholen wir, bis wir wieder entweder zu einer geringen Anzahl von Zahlen kommen, welche wir in V ausprobieren müssen. Als Lösungen wählen wir diejenigen x, für welche V ein Quadrat wird, auch hier ist, wenn alle Zahlen aus ω der Form

$$Dt \pm r_1,\ Dt \pm r_2, \ldots$$

herausfallen, ein Beweis dafür, daß die gegebene Gleichung keine Lösungen hat. Diese Auflösungen der Gleichung

$$x^2 + Dy^2 = k$$

werden wir durch ein Beispiel erläutern.

Beispiel: Es sei

$$x^2 + 43y^2 = 3517669$$

$$\left[\sqrt{\frac{3517669}{43}}\right] = \left[\sqrt{81806}\right] = 286$$

also zuerst besteht ω aus 287 Zahlen.

Setzen wir $E_1 = 3$, so sind 0, 1, Reste, 2 Nichtrest. Die Wurzel der Kongruenz

$$43z \equiv 3517669 - 2 \pmod 3$$

ist 2, also Nichtrest und infolgedessen kann 3 als E_1 nicht benutzt werden.

Setzen wir $E_1 = 4$, so sind 0, 1, Reste; 2, 3, Nichtreste. Die Kongruenz

$$43z \equiv 3517669 - 2 \pmod 4$$

bietet die Lösung 1. Die Kongruenz

$$43z \equiv 3517669 - 3 \pmod 4$$

die Lösung 2. Die Zahl 1 ist quadratischer Rest und kann als α_1 betrachtet werden. Die Kongruenz

$$y^2 \equiv 1 \pmod 4$$

bietet die Lösung $h_1 = \pm 1$, demnach sind alle Zahlen der Form $4t \pm 1$ d. h. alle 143 ungeraden Zahlen aus ω wegzulassen. Die Probeanzahl ist auf die Hälfte verkleinert. Die übrigen Zahlen aus ω werden wir in derselben Weise weiter auszuschließen versuchen.

Setzen wir $E_2 = 5$, so sind 0, 1, 4 Reste, 2, 3 Nichtreste. Die Kongruenz

$$43z \equiv 3517669 - 2 \pmod 5$$

bietet $\alpha_1 = 4$. Die Kongruenz

$$y^2 \equiv 4 \pmod 5$$

hat die Lösung $h_1 = \pm 2$, also fallen alle Zahlen der Form $5t \pm 2$, d. h. die folgenden 57 Zahlen

2, 8, 12, 18, 22, 28, 32, 38, 42, 48, 52, 58, 62, 68, 72, 78, 82, 88, 92, 98, 102, 108, 112, 118, 122, 128, 132, 138, 142, 148, 152, 158, 162, 168, 172, 178, 182, 188, 192, 198, 202, 208, 212, 218, 222, 228, 232, 238, 242, 248, 252, 258, 262, 268, 272, 278, 282

aus.

Die Zahl $E_3 = 6$ bietet keine h und kann also nicht als E_3 benutzt werden. Für die Zahl 7 sind 3, 5, 6 Nichtreste und 7 bietet $\alpha_1 = 2$ und $h_1 = \pm 3$, also sind auch die Zahlen der Form $7t \pm 3$ auszuschließen und es fallen die folgenden 25 Zahlen

4, 10, 24, 46, 60, 66, 74, 80, 94, 116, 130, 136, 144, 150, 164, 186, 200, 206, 214, 220, 234, 256, 270, 276, 284

aus.

Setzen wir $E_4 = 8$, so sind 2, 3, 5, 6, 7 Nichtreste, wir bekommen

$$\alpha_1 = 1, \quad h_1 = \pm 1, \quad h_2 = \pm 3,$$

also alle Zahlen der Form $8t \pm 1$ und $8t \pm 3$ sind auszuschließen, sie sind aber schon ausgeschlossen durch die Form $4t \pm 1$.

Setzen wir $E_4 = 9$, so sind 2, 3, 5, 6, 8 Nichtreste,

$$\alpha_1 = 1, \quad \alpha_2 = 7, \quad h_1 = \pm 1, \quad h_2 = \pm 4,$$

also sind auch die Zahlen der Form $9t \pm 1$, und $9t \pm 4$ auszuschließen und es fallen auch die folgenden 26 Zahlen

14, 26, 40, 44, 50, 64, 76, 86, 100, 104, 134, 140, 154, 166, 170, 176, 184, 190, 194, 224, 226, 230, 244, 260, 266, 274, 280

aus.

Es bleiben noch die folgenden 32 Zahlen

0, 6, 16, 20, 30, 34, 36, 54, 56, 70, 84, 90, 96, 106, 110, 120, 124, 126, 146, 156, 160, 174, 196, 204, 210, 216, 236, 240, 250, 254, 264, 286

übrig.

Setzen wir $E_5 = 10$, so ist $\alpha_1 = 9$, $\alpha_2 = 4$, $h_1 = \pm 3$, $h_2 = \pm 2$, also fallen auch die Zahlen $10t \pm 3$ und $10t \pm 2$ aus. Die ersten sind aber schon als ungerade ausgeschlossen, auch die zweiten sind schon durch die Form $5t \pm 2$ ausgeschlossen.

Setzen wir $E_5 = 11$, so sind 2, 6, 7, 8, 10 Nichtreste,

$$\alpha_1 = 1, \quad \alpha_2 = 5, \quad \alpha_3 = 9, \; h_1 = \pm 1, \quad h_2 = \pm 4, \quad h_3 = \pm 3,$$

also fallen auch die Zahlen der Form $11t \pm 1$, $11t \pm 4$, $11t \pm 3$ aus, das sind die folgenden 19 Zahlen

30, 34, 36, 54, 56, 70, 84, 96, 106, 114, 120, 124, 146, 180, 210, 216, 246, 250, 254.

Es bleiben noch die Zahlen

0, 6, 16, 20, 90, 110, 126, 156, 174, 196, 204, 236, 240, 264, 286.

Setzen wir $E_6 = 12$, so sind 2, 3, 5, 6, 7, 8, 10, 11 Nichtreste,

$$\alpha_1 = 1, \quad \alpha_2 = 9, \quad h_1 = \pm 1, \quad h_2 = \pm 5, \quad h_3 = \pm 3,$$

die Zahlen $12t \pm 1$, $12t \pm 5$, $12t \pm 3$ als ungerade kommen aber nicht in Betracht.

Setzen wir $E_6 = 13$, so sind 2, 5, 6, 7, 8, 11 Nichtreste,

$$\alpha_1 = 9, \quad \alpha_2 = 1, \quad \alpha_3 = 10, \quad h_1 = \pm 1, \quad h_2 = \pm 3, \quad h_3 = \pm 6.$$

Die Zahlen $13t \pm 1$, $13t \pm 3$, $13t \pm 6$ fallen wieder aus. Das sind die folgenden 7 Zahlen

6, 16, 20, 90, 110, 196, 240.

Setzen wir $E_7 = 17$, so sind 3, 5, 6, 7, 10, 11, 12, 14 Nichtreste,

$$\alpha_1 = 1, \quad \alpha_2 = 4, \quad \alpha_3 = 0, \quad \alpha_4 = 13, \quad \alpha_5 = 2,$$

$$h_1 = \pm 1, \quad h_2 = \pm 2, \quad h_3 = \pm 0, \quad h_4 = \pm 8, \quad h_5 = \pm 6,$$

und damit sind die Zahlen der Form $17t \pm 1$, $17t \pm 2$, $17t$, $17t \pm 8$, $17t \pm 6$ auszuschließen. Es fallen auch die Zahlen

0, 204, 236, 264,

aus.

Für $E_8 = 19$ sind die Zahlen 2, 3, 8, 10, 12, 13, 14, 15, 18 Nichtreste, $\alpha_1 = 9$, $\alpha_2 = 5$, $\alpha_3 = 4$, $\alpha_4 = 7$,

$$h_1 = \pm 3, \quad h_2 = \pm 9, \quad h_3 = \pm 2, \quad h_4 = \pm 8,$$

es sind auch die Zahlen der Form $19t \pm 3$, $19t \pm 9$, $19t \pm 2$, $19t \pm 8$ auszuschließen, es fallen dadurch die Zahlen

160, 174

aus und es bleiben noch die folgenden 3 Zahlen

126, 156, 286

übrig.

Diese 3 Zahlen probieren wir mittels des Ausdruckes V aus. Es zeigt sich, daß

$$V = 3517669 - 43\,(286)^2 = (21)^2,$$

also $y = 286$, $x = 21$ ist ein Lösungspaar der Gleichung

$$x^2 + 43y^2 = 3517669$$

und das ist zugleich das einzige Lösungspaar der zu untersuchenden Gleichung.

Dieses Beispiel

$$x^2 + 43y^2 = 3517669$$

werden wir auch mittels der zweiten Methode untersuchen

$$[\sqrt{3517669}] = 1875,$$

also enthält ω_1 alle ganzen rationalen Zahlen von 0 bis 1875, d. h. 1876 Zahlen.

Für die Kongruenz

$$x \equiv 3517669 \pmod{43}$$

ist $\delta \equiv 11 \pmod{43}$ die Wurzel.

Die Wurzel der Kongruenz

$$x^2 \equiv 11 \pmod{43}$$

ist ± 21, also brauchen wir in ω_1 nur die Zahlen der Form

$$43t \pm 21$$

zu untersuchen. Das sind nur 87 Zahlen. Die übrigen 1789 Zahlen sind damit ausgeschlossen.

Wir setzen $E = 3$, dann ist 2 Nichtrest. Die Wurzel der Kongruenz

$$z \equiv 3517669 - 2 \cdot 43 \pmod{3}$$

ist 2, also bietet $E_1 = 3$ keine Ausschließung.

Setzen wir $E_1 = 4$, so sind 2, 3 die Nichtreste. Als Wurzel der Kongruenz

$$z \equiv 3517669 - 2 \cdot 43 \pmod{4}$$

erhalten wir die Zahl 3, als Wurzel der Kongruenz

$$z \equiv 3517669 - 3 \cdot 43 \pmod{4}$$

die Zahl 0, also $\alpha_1 = 0$. Die Wurzeln der Kongruenz

$$x^2 \equiv 0 \pmod{4}$$

sind die Zahlen 0 und ± 2, also ist $h_1 = 0$, $h_2 = \pm 2$ und die Zahlen $4t$ und $4t \pm 2$ sind auszuschließen. Damit sind alle gerade Zahlen ausgeschlossen. Es muß also in dem Ausdruck

$$43t \pm 21$$

t eine gerade Zahl sein, infolgedessen sind alle zu untersuchende Zahlen in der Form

$$43 \cdot 2t \pm 21$$

enthalten. Das sind die folgenden 44 Zahlen

21, 65, 107, 151, 193, 237, 279, 323, 365, 409, 451, 495, 537, 581, 623, 667, 709, 753, 795, 839, 881, 925, 967, 1011, 1053, 1097, 1139, 1183, 1225, 1269, 1355, 1361, 1397, 1441, 1483, 1527, 1569, 1613, 1655, 1699, 1741, 1785, 1827, 1871.

Die übrigen 43 Zahlen sind ausgeschlossen.

Setzen wir $E_2 = 5$, so sind 2, 3 Nichtreste, $\alpha_1 = 0$, $h_1 = 0$, also sind alle Zahlen der Form $5t$ auszuschließen, damit sind die folgenden 9 Zahlen

65, 365, 495, 795, 925, 1225, 1355, 1655, 1785

ausgeschlossen.

$E = 6$ bietet keine Ausschließungen. Für $E_3 = 7$ und für die weiter benutzten E werden wir die Nichtreste nicht angeben, weil sie schon angegeben sind. Wir benutzen E aus der natürlichen Zahlenreihe nacheinander, obwohl das nicht nötig ist.

Sei $E_3 = 7$, so ist $\alpha_1 = 2$, $h_1 = \pm 3$, folglich sind die Zahlen der Form $7t \pm 3$ auszuschließen. Das sind die folgenden 10 Zahlen

151, 193, 237, 409, 451, 753, 1011, 1053, 1397, 1613.

$E = 8$ bietet $\alpha_1 = 4$, $\alpha_2 = 0$, $h_1 = \pm 2$, $h_2 = 0$, $h_3 = \pm 4$ die Zahlen $8t \pm 2$, $8t$, $8t \pm 4$ sind schon als gerade ausgeschlossen.

Für $E_4 = 9$ ist $\alpha_1 = 7$, $\alpha_2 = 4$, $h_1 = \pm 4$, $h_2 = \pm 2$, also auch die Zahlen $9t \pm 4$, $9t \pm 2$ sind auszuschließen und dadurch fallen auch die folgenden 10 Zahlen

581, 623, 709, 839, 967, 1139, 1183, 1483, 1699, 1741

aus.

$E = 10$ bietet keine Ausschließungen. Eür $E_5 = 11$ ist

$$\alpha_1 = 3, \quad \alpha_2 = 9, \quad \alpha_3 = 0, \quad h_1 = \pm 5, \quad h_2 = \pm 3, \quad h_3 = 0,$$

also $11t \pm 5$, $11t \pm 3$, $11t$ sind auszuschließen und damit sind auch die 3 Zahlen

107, 1097, 1441

ausgeschlossen. Es bleiben noch die folgenden 12 Zahlen

21, 279, 323, 537, 667, 881, 1269, 1311, 1527, 1569, 1827, 1871

übrig.

$E = 12$ bietet keine Ausschließungen. Für $E_6 = 13$ ist

$$\alpha_1 = 1, \quad \alpha_2 = 10, \quad h_1 = \pm 1, \quad h_2 = \pm 6,$$

also sind auch die Zahlen $13t \pm 1$, $13t \pm 6$ auszuschließen. Es fallen dadurch die 4 Zahlen

279, 1527, 1827, 1871

aus.

Für $E_7 = 17$ ist

$$\alpha_1 = 2, \quad \alpha_2 = 1, \quad \alpha_3 = 9, \quad \alpha_4 = 0, \quad \alpha_5 = 15,$$
$$h_1 = \pm 6, \quad h_2 = \pm 1, \quad h_3 = \pm 3, \quad h_4 = 0, \quad h_5 = \pm 7,$$

auch alle Zahlen der Form $17t \pm 6$, $17t \pm 1$, $17t \pm 3$, $17t$, $17t \pm 7$ sind auszuschließen. Dadurch fallen noch die folgenden 4 Zahlen

323, 537, 881, 1269

aus.

Für $E_8 = 19$ ist

$$\alpha_1 = 7, \quad \alpha_2 = 16, \quad \alpha_3 = 6, \quad \alpha_4 = 1,$$
$$h_1 = \pm 8, \quad h_2 = \pm 4, \quad h_3 = \pm 5, \quad h_4 = \pm 1,$$

also sind auch alle Zahlen der Form $19t \pm 8$, $19t \pm 4$, $19t \pm 5$, $19t \pm 1$ auszuschließen; es fällt dadurch auch die Zahl

$$1569$$

aus und es bleiben noch übrig 3 Zahlen, nämlich

$$21,\ 667,\ 1311.$$

Aus diesen Zahlen ergibt nur die Zahl 21, mittels des Ausdruckes

$$V = \frac{3517669 - (21)^2}{43} = (286)^2$$

ausprobiert, ein Quadrat, also, wie schon bekannt, ist $x = 21$, $y = 286$ das einzige Lösungspaar.

§ 7. Die Faktorenzerlegung der quadratischen Form $a^2 + Db^2$.

Auch die Zerlegung in rat. Faktoren der rat. Zahl $N(m + n\varrho)$ oder der quadratischen Form $\frac{a^2 + Db^2}{4}$, allerdings nur bei der Bestimmung der ungeraden Faktoren, bietet große Schwierigkeiten, wenn $a^2 + Db^2$ sehr groß ist. Diese Schwierigkeiten werden wir dadurch beseitigen, daß wir die linearen Formen für die ungeraden Teiler der quadratischen Form

$$a^2 + Db^2$$

angeben.[1])

Wir werden dabei nur den Fall erledigen, wo a und b relativprim sind, weil gerade das bei unseren Untersuchungen der Fall ist, und aus demselben Grund werden wir für D einen Wert der Reihe

$$1, 2, 3, 7, 11, 19, 27, 43, 67, 163$$

beibehalten.

Hier ist nur 27 eine zusammengesetzte Zahl. Die Form $a^2 + 27b^2$ kann man aber als $a^2 + 3(3b)^2$ betrachten, für D die Zahl 3 annehmen.

Dadurch wird jede Zahl D, mit welcher wir zu tun haben eine Primzahl.

Diese Beschränkungen werden unsere Aufgabe wesentlich vereinfachen. Zuerst werden wir den folgenden Satz beweisen.

Satz I: *Hat die Kongruenz*

$$x^2 + Dy^2 \equiv 0 \pmod{p}$$

eine Lösung x, y, wo x und y relativ prim sind, so hat auch die Kongruenz

$$u^2 + D \equiv 0 \pmod{p}$$

eine Lösung.

Beweis: Da x und y relativ prim sind, so sind auch y und p relativ prim, also hat die Kongruenz

$$yu \equiv x \pmod{p}$$

eine Lösung. Aus dieser Kongruenz folgt

$$y^2u^2 \equiv x^2 \pmod{p},$$

was zusammen mit der Kongruenz

$$x^2 + Dy^2 \equiv 0 \pmod{p}$$

---

1) Tschebyschew, „Th. d. Kongr.“, §§ 42—44.

die Kongruenz

$$y^2u + Dy^2 \equiv 0 \pmod{p}$$

ergibt, da aber y und p relativ prim sind, so kann man y^2 kürzen und wir bekommen

$$u^2 + D \equiv 0 \pmod{p}$$

oder im Legendreschen Symbol ausgedrückt

$$\left(\frac{-D}{p}\right) = 1.$$

Satz 2: *Wenn umgekehrt diese Kongruenz erfüllt ist, so werden wir immer eine Lösung der Kongruenz*

$$x^2 + Dy^2 \equiv 0 \pmod{p}$$

finden können. Wir setzen nämlich

$$y = 1, \quad x = u.$$

Schon auf Grund dieses Satzes kann man immer feststellen, ob eine gegebene quadratische Form $a^2 + Db^2$ Teiler hat oder nicht. Wir werden diesen Satz benutzen, um nicht nur die Möglichkeit der Zerlegung zu beweisen, sondern auch die Zerlegung selbst anzugeben. Das erreichen wir dadurch, daß wir die linearen Formen der Zahlen p, welche Teiler der Form $a^2 + Db^2$ sind, für alle ungeraden p bestimmen und, da jede ganze rationale Zahl p als lineare Form betrachtet werden kann, so werden dies alle Teiler sein.

Ist $p = 2$, so ist p ein Teiler der Form $a^2 + Db^2$ bei ungeradem D, wenn a und b beide zugleich ungerade sind und zwar nur in diesem Fall, denn a und b sind relativ prim.

Die Ausschließung des Teilers 2^ν bietet keine Schwierigkeiten. Wenn $a = Da_1$ ist, so ist ein Faktor D vorhanden. Dividieren wir $a^2 + Db^2 = a_1{}^2D^2 + Db^2$ durch D, so bekommen wir $b^2 + Da_1{}^2$ also dieselbe Form, aber vom Faktor D befreit.

Wir betrachten jetzt die anderen ungeraden Zahlen p. Diese lassen sich auf Grund der folgenden zwei Sätze bestimmen.

Satz 3: *Alle ungeraden Teiler der Zahl $a^2 + 2b^2$ sind in der Form $8t + 1$ oder $8t + 3$ enthalten.*

Beweis: Ist p ein ungerader Teiler der Zahl $a^2 + 2b^2$, so ist

$$a^2 + 2b^2 \equiv 0 \pmod{p},$$

also hat die Kongruenz

$$u^2 + 2 \equiv 0 \pmod{p}$$

eine Lösung (Satz 1), d. h.

$$\left(\frac{-2}{\alpha}\right) = 1, \ \left(\frac{-2}{\beta}\right) = 1, \ \left(\frac{-2}{\gamma}\right) = 1, \ldots,$$

wo $\alpha, \beta, \gamma, \ldots$ alle Primfaktoren der Zahl p sind. Wir werden jetzt die Form dieser Zahlen untersuchen.

$$\left(\frac{-2}{\alpha}\right) = \left(\frac{2}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}} = (-1)^{\frac{-\alpha^2-1}{8}}(-1)^{\frac{\alpha-1}{2}} = -(-1)^{\frac{-\alpha^2+4\alpha-3}{8}}.$$

Setzen wir die ungerade Zahl $\alpha = 8t+1, 8t+3, 8t+5, 8t+7$, so ist

$$\left(\frac{-2}{8t+1}\right) = 1, \left(\frac{-2}{8t+3}\right) = 1, \left(\frac{-2}{8t+5}\right) = -1, \left(\frac{-2}{8t+7}\right) = -1.$$

Die Zahl α kann also nur die Form $8t+1$ oder $8t+3$ haben, also hat p die Form $8P + 3^\lambda$ und weil 3^λ die Form $8t+1$ oder $8t+3$ hat, so ist damit der Satz bewiesen.

Satz 4: *Ist D eine Primzahl der Form $4n+3$ und p ein ungerader Teiler der Zahl $a^2 + Db^2$, so ist*

$$\left(\frac{p}{D}\right) = +1.$$

Beweis: Ist p ein Teiler von $a^2 + Db^2$, so ist

$$a^2 + Db^2 \equiv 0 \pmod{p},$$

dann hat aber die Kongruenz

$$u^2 + D \equiv 0 \pmod{p}$$

eine Lösung (Satz 1).

Seien $\alpha, \beta, \gamma,$ die Primteiler von p, so ist dann

$$\left(\frac{-D}{\alpha}\right) = 1, \left(\frac{-D}{\beta}\right) = 1, \left(\frac{-D}{\gamma}\right) = 1, \ldots$$

Aus diesen Kongruenzen lassen sich auch

$$\left(\frac{\alpha}{D}\right), \left(\frac{\beta}{D}\right), \ldots$$

bestimmen auf Grund vom Satz

$$\left(\frac{\alpha}{D}\right) = \left(\frac{D}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{D-1}{2}} = \left(\frac{-D}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{\alpha-1}{2}+\frac{\alpha-1}{2}\cdot\frac{D-1}{2}} =$$

$$= \left(\frac{-D}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{D+1}{2}}.$$

Da $\left(\frac{-D}{\alpha}\right) = 1$ und D die Form $4n+3$ hat, so folgt aus dieser Gleichung

$$\left(\frac{\alpha}{D}\right) = 1$$

zugleich aber auch, daß

$$\left(\frac{\beta}{D}\right) = 1, \left(\frac{\gamma}{D}\right) = 1, \ldots$$

Durch Multiplikation dieser Gleichungen erhalten wir:

$$\left(\frac{\alpha}{D}\right)\left(\frac{\beta}{D}\right)\left(\frac{\gamma}{D}\right)\ldots = \left(\frac{\alpha\beta\gamma\ldots}{D}\right) = \left(\frac{p}{D}\right) = 1$$

q. e. d.

Satz 5: *Ist D eine Primzahl der Form $4n+1$ und p ein Teiler von a^2+Db^2, so ist* $\left(\frac{p}{D}\right) = (-1)^{\frac{p-1}{2}}$ *d. h.* $\left(\frac{p}{D}\right) = 1$, *wenn* $p = 4m+1$ *und* $\left(\frac{p}{D}\right) = -1$, *wenn* $p = 4m+3$ *ist.*

Beweis: Ist p ein Teiler von a^2+Db^2, so ist

$$a^2 + Db^2 \equiv 0 \pmod{p};$$

also hat die Kongruenz

$$u^2 + D \equiv 0 \pmod{p}$$

eine Lösung, folglich sind

$$\left(\frac{-D}{\alpha}\right) = 1, \left(\frac{-D}{\beta}\right) = 1, \ldots$$

wo $\alpha, \beta, \gamma, \ldots$ wieder Primzahlen sind, welche in p aufgehen.

Es ist wie früher

$$\left(\frac{\alpha}{D}\right) = \left(\frac{-D}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{D+1}{2}};$$

da aber

$$\left(\frac{-D}{\alpha}\right) = 1 \text{ ist, so ist}$$

$$\left(\frac{\alpha}{D}\right) = (-1)^{\frac{\alpha-1}{2}\cdot\frac{D+1}{2}}.$$

Wir haben $D = 4m+1$ angenommen, folglich ist

$$(-1)^{\frac{\alpha-1}{2}\cdot\frac{D+1}{2}} = (-1)^{\frac{\alpha-1}{2}\cdot\frac{4m+2}{2}} = (-1)^{\frac{\alpha-1}{2}(2m+1)}$$

$$= (-1)^{\frac{\alpha-1}{2}\cdot 2m} \cdot (-1)^{\frac{\alpha-1}{2}} = (-1)^{\frac{\alpha-1}{2}},$$

also ist

$$\left(\frac{\alpha}{D}\right) = (-1)^{\frac{\alpha-1}{2}},$$

ebenfalls

$$\left(\frac{\beta}{D}\right) = (-1)^{\frac{\beta-1}{2}}, \left(\frac{\gamma}{D}\right) = (-1)^{\frac{\gamma-1}{2}}, \ldots$$

Durch Multiplikation bekommen wir

$$\left(\frac{\alpha}{D}\right)\left(\frac{\beta}{D}\right)\left(\frac{\gamma}{D}\right)\ldots = \left(\frac{p}{D}\right) = (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\cdots} = (-1)^{\frac{p-1}{2}};$$

denn die Zahlen $\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \ldots$ und $\frac{p-1}{2}$ unterscheiden sich nur durch eine gerade Zahl. In der Tat

$$\frac{p-1}{2} = \frac{\alpha\beta\gamma\ldots-1}{2} = \frac{-1+\left(1+2\frac{\alpha-1}{2}\right)\left(1+2\frac{\beta-1}{2}\right)\cdots}{2}$$

Wenn wir hier aber die Multiplikation ausführen und die Glieder, welche 2 enthalten, ausschließen, so bleibt

$$\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \cdots$$

und also

$$\left(\frac{p}{D}\right) = (-1)^{\frac{p-1}{2}}.$$

Ist $p = 4m + 1$, so ist

$$\left(\frac{p}{D}\right) = (-1)^{2m} = 1.$$

Ist $p = 4m + 3$, so ist

$$\left(\frac{p}{D}\right) = (-1)^{2m+1} = -1$$

q. e. d.

Auf Grund dieser Sätze lassen sich ohne Schwierigkeiten alle ungeraden Teiler der Form $a^2 + Db^2$ finden, wenn D eine ungerade Primzahl ist. Diese Teiler werden bestimmt durch eine der Kongruenzen:

$$\text{(1)} \qquad \left(\frac{p}{D}\right) = 1 \text{ und } \left(\frac{p}{D}\right) = -1,$$

je nachdem ob D die Form $4m + 3$ oder $4m + 1$ hat und je nachdem, ob $p = 4m + 1$ oder $4m + 3$ ist. Die Zahlen p, welche diese Kongruenz erfüllen, sind bekanntermaßen für die erste Kongruenz

$$p = a_1 + nD,\ p = a_2 + nD,\ \ldots,\ p = a_{\frac{D-1}{2}} + nD,$$

wo n eine beliebige Zahl ist und

$$a_1,\ a_2,\ \ldots,\ a_{\frac{D-1}{2}}$$

Reste von den Divisionen

$$1^2,\ 2^2,\ 3^2,\ \ldots \left(\frac{D-1}{2}\right)^2$$

durch D sind. Die Lösungen der zweiten Kongruenz (1) werden bestimmt durch die Ausdrücke

$$p = b_1 + nD,\ p = b_2 + nD,\ \ldots,\ p = b_{\frac{D-1}{2}} + nD,$$

wo

$$b_1,\ b_2,\ \ldots,\ b_{\frac{D-1}{2}}$$

diejenigen von den Zahlen 1, 2, 3, ..., $(D - 1)$ darstellen, welche nicht $a_1, a_2, \ldots, a_{\frac{D-1}{2}}$ sind.

Jetzt werden wir noch untersuchen, wann jede dieser Zahlen p eine Zahl von der Form $4m + 1$ und wann von der Form $4m + 3$ wird.

Ist

$$a_\lambda + nD = 4m + 1,$$

so ist

$$a_\lambda + nD \equiv 1 \pmod 4 \text{ oder } nD \equiv 1 - a_\lambda \pmod 4.$$

Da D ungerade ist, so hat diese Kongruenz immer eine Lösung, nämlich

$$n \equiv D(1 - a_\lambda) \pmod 4,$$

welche einen der Werte 0, 1, 2, 3 haben kann. Bezeichnen wir sie mit r, so ist

$$r \equiv D(1 - a_\lambda) \pmod 4$$

und die vorhergehende Kongruenz bekommt die Form

$$n \equiv r \pmod 4,$$

also $n = 4t + r$, folglich

$$p = nD + a_\lambda = 4Dt + Dr + a_\lambda.$$

In ähnlicher Weise lassen sich auch die Zahlen $nD + a_\lambda$ bestimmen, welche die Form $4m + 3$ haben. Das sind die Zahlen der Form

$$p = 4Dt + Dr_1 + a_\lambda,$$

wo r_1 die kleinste Zahl ist, welche die Kongruenz

$$n \equiv D(3 - a) \pmod 4$$

erfüllt. Da diese Unterscheidung nur in dem Fall $D = 1$ eine Rolle spielt, so betrachten wir für alle übrigen D die Zahlen $p = 4m + 1$ und $= 4m + 3$ als Zahlen der Form $2m + 1$. Dann ist

$$a_\lambda + Dn = 2m + 1,$$

d. h.

$$nD + a_\lambda \equiv 1 \pmod 2$$

oder

$$nD \equiv 1 - a_\lambda \pmod 2.$$

Ist a_λ ungerade, so ist diese Kongruenz durch $n = 0$ erfüllt, also sind ihre Lösungen

$$n \equiv 0 \pmod 2,$$

also $n = 2t$, ist dagegen a_λ gerade, so wird diese Kongruenz durch $n = 1$ erfüllt, weil D ungerade ist und es ist also

$$n = 2t + 1.$$

Diese Werte, in die Form $p = nD + a$ eingesetzt, ergeben $p = 2Dt + a_\lambda$ und $p = 2Dt + D + a$, je nachdem a_λ gerade oder ungerade ist.

Beispiel: Es seien alle ungeraden Faktoren von

$$a^2 + 19b^2$$

zu bestimmen. Da 19 eine Primzahl der Form $4m + 3$ ist, so werden wir das folgendermaßen erreichen.

Wir lösen zuerst die Kongruenz

$$\left(\frac{p}{19}\right) = 1$$

auf.

Wie dividieren zu diesem Zwecke alle Zahlen

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ 9^2$$

durch 19. Die Reste sind

$$1,\ 4,\ 9,\ 16,\ 6,\ 17,\ 11,\ 7,\ 5,$$

also sind alle p, welche der Kongruenz $\left(\frac{p}{19}\right) = 1$ genügen, die folgenden

$$19t+1,\ 19t+4,\ 19t+9,\ 19t+16,\ 19t+6,\ 19t+17,\ 19t+11,$$
$$19t+7,\ 19t+5.$$

Da aber diese p alle ungerade sein sollen, so setzen wir, wie gezeigt, statt $19t+1$ die Form $19 \cdot 2t + 1$, statt $19t+4$ die Form $19 \cdot 2t + 19 + 4$ usw.

Alle ungeraden linearen Teiler dieser Form sind also

$$38t+1,\ 38t+5,\ 38t+7,\ 38t+9,\ 38t+11,\ 38t+17,\ 38t+23,$$
$$38t+25,\ 38t+35.$$

Es sollen z. B. die Faktoren der Form

$$378^2 + 19 \cdot 43^2 = 178015$$

bestimmt werden.

$$178015 = 5 \cdot 35603.$$

Die Zahl 35603 ist eine Primzahl. Das kann man durch Ausprobieren mit $[\sqrt{35603}] = 188$ Zahlen feststellen. Wenn wir aber die Formen der linearen Teiler benutzen, so brauchen wir nur $\left[\frac{188}{38}\right] \cdot 9 = 4 \cdot 9 = 36$ Zahlen auszuprobieren; haben wir die Möglichkeit, nur die Primzahlen in dem Intervall von 1 bis 188 zu probieren, so sind das 42 Zahlen. Mit Benutzung obiger Formen bleiben aber nur 17.

Es wäre zweckmäßig die linearen Formen der für uns wichtigen quadratischen Formen alle in einer Tabelle anzugeben. Die Teiler 2^ν und D sind in besagter Weise zuerst auszuschließen.

Tabelle der linearen Faktoren der quadratischen Formen $a^2 + Db^2$.

$$D = 1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 27,\ 43,\ 67,\ 163.$$

Die linearen Faktoren für $a^2 + b^2$ sind

$$4t+1;$$

für $a^2 + 2b^2$ sind

$$8t+1, 3;$$

für $a^2 + 3b^2$ sind

$$6t+1;$$

für $a^2 + 7b^2$ sind

$$14t + 1, 9, 11;$$

für $a^2 + 11b^2$ sind

$$22t + 1, 3, 5, 9, 15;$$

für $a^2 + 19b^2$ sind

$$38t + 1, 5, 7, 9, 11, 17, 23, 25, 35;$$

für $a^2 + 27b^2$ sind ebenso wie für $a^2 + 3b^2$ wieder

$$6t + 1;$$

für $a^2 + 43b^2$ sind

$86t + 1$, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81, 83;

für $a^2 + 67b^2$ sind

$134t + 1$, 9, 15, 17, 19, 21, 23, 25, 29, 33, 35, 37, 39, 47, 49, 55, 59, 65, 71, 73, 77, 81, 83, 89, 91, 93, 103, 107, 121, 123, 127, 129, 131;

für $a^2 + 163b^2$ sind

$326t + 1$, 9, 15, 21, 25, 33, 35, 39, 41, 43, 47, 49, 51, 53, 55, 57, 61, 65, 69, 71, 77, 81, 83, 85, 87, 91, 93, 95, 97, 111, 113, 115, 119, 121, 131, 133, 135, 143, 145, 151, 155, 161, 167, 169, 173, 177, 179, 185, 187, 189, 197, 199, 201, 203, 209, 217, 219, 221, 223, 225, 227, 237, 247, 251, 253, 259, 263, 267, 281, 289, 295, 297, 299, 303, 307, 309, 313, 315, 319, 321, 323.

Kurze Zusammenstellung des Inhaltes.

§ 1. Die quadratischen imaginären Zahlen.

Die Einheiten eines Körpers sind in der Form

$$\varepsilon = \delta \varepsilon_1^{l_1} \varepsilon_2^{l_2} \cdots \varepsilon_{\nu-1}^{l_{\nu-1}}$$

enthalten.

Der einfachste Fall $\nu = 1$ tritt bei den imaginären quadratischen Körpern ein. Für diese Körper läßt sich neben dem einfachsten Ausdruck auch die Anzahl der Einheiten genau angeben.

Die ganzen Zahlen eines quadratischen Körpers sind in der Form $\frac{a \pm b\varrho}{2}$ enthalten.

Dieser Satz ist nur teilweise umkehrbar, nämlich $\frac{a \pm b\varrho}{2}$ ist eine ganze Zahl, nur wenn $\frac{a^2 + Db^2}{4}$ ganz ist.

Ist die Zahl $\frac{a \pm b\varrho}{2}$ ganz, so sind a und b beide zugleich gerade oder ungerade.

Die Zahlen $\frac{a \pm b\varrho}{2}$, wo a und b beide ungerade sind, sind nur ganz, wenn $\frac{1 + D}{4}$ eine ganze rationale Zahl ist.

Ist $\frac{a^2 + Db^2}{4} = 1$ so sind die Zahlen $\frac{a + b\varrho}{2}$ und $\frac{a - b\varrho}{2}$ Einheiten und umgekehrt.

Ist $D > 4$ oder $D = 2$, so gibt es in diesen Körpern nur die zwei Einheiten ± 1, ist $D = 1$, so findet man 4 Einheiten ± 1, $\pm i$, ist $D = 3$, so sind ± 1, $\pm \frac{-1 + i\sqrt{3}}{2}$; $\pm \frac{-1 + \sqrt{-3}}{2}$ die 6 Einheiten dieses Körpers.

Die Sätze der Teilbarkeit, welche für ganze rationale Zahlen gelten, sind für die algebraischen nicht alle gültig. Es ist nämlich die Eindeutigkeit der Zerlegung in unzerlegbare Faktoren nicht immer erfüllt; aber auch selbst wenn die Gesetze der Teilbarkeit von ganzen rationalen Zahlen auch in bestimmten algebraischen Körpern richtig bleiben, so müssen wir doch ein Mittel haben, alle nicht wesentlich verschiedenen Zahlen zusammenfassen zu können. Dieses Mittel bilden die Ideale.

Eine endliche Anzahl von Einheiten haben nur, wie gezeigt, die imaginären quadratischen Körper. Unter denselben sind die mit den Diskriminanten

$$-1, -2, -3, -7, -11, -19, -27, -43, -67, -163$$

eindeutig zerlegbar. Die Ideale sind für diese Körper als solche überflüssig und es ist für diese Körper ein Mittel anzugeben den größten gem. Teiler ohne Benutzung der Ideale zu finden.

§ 2. Die Normen der quadratischen imaginären Zahlen und der Begriff „Größter gemeinschaftlicher Teiler" dieser Zahlen.

Jeder Zahl $m + n\varrho$ ist die Norm $m^2 + Dn^2$ eindeutig zugeordnet.

Die Norm eines Produktes ist gleich dem Produkt der Normen der einzelnen Faktoren.

Die Norm eines Quotienten ist gleich dem Quotient der Normen von Zähler und Nenner.

$N(m + n\varrho)$ ist eine ganze positive Zahl.

Ist $N(m + n\varrho) = 0$, so muß $m = 0$ und $n = 0$ sein.

Wir werden die Zahl $m + n\varrho$ normgrößer als $r + s\varrho$ nennen, wenn $m^2 + Dn^2 > r^2 + Ds^2$, normkleiner wenn $m^2 + Dn^2 < r^2 + Ds^2$ und normgleich wenn $m^2 + Dn^2 = r^2 + Ds^2$ ist. Normgleich können auch verschiedene Zahlen sein. $m + n\varrho$ ist $= r + s\varrho$ nur wenn $m = r$ und $n = s$ ist.

Ist $N(m + n\varrho) = 0$ so ist $m + n\varrho = 0$.

Es gibt zusammengesetzte Zahlen.

Derjenige gemeinsame Teiler, welcher durch alle anderen gemeinsamen Teiler teilbar ist, wird als größter gemeinschaftlicher Teiler bezeichnet und wird symbolisch dargestellt in der Form

$$G(m_1 + n_1\varrho,\ m_2 + n_2\varrho, \ldots) = x + y\varrho$$

$G(m_1 + n_1\varrho, \ldots)$ ist eindeutig. Ist $z + w\varrho$ eine Einheit, so sind die Zahlen $m_1 + n_1\varrho, \ldots$ teilerfremd.

Die Gleichung $A = BQ + R$, wo $R < B$ ist, bleibt für die zu untersuchenden Zahlen nicht unbedingt erhalten. Da der Euklidische Algorithmus gerade auf dieser Eigenschaft beruht, so muß zuerst die Möglichkeit der Bildung dieser Gleichung untersucht werden.

§ 3. Der Euklidische Algorithmus für eindeutig zerlegbare quadratische Zahlen mit negativer Diskriminante.

Jede ganze quadratische Zahl $m + n\varrho$ läßt sich auf die Form $a + b\sigma$ wo a, b ganze Zahlen und σ eine ganze Zahl desselben Körpers ist, bringen und umgekehrt.

Ist auch σ_1 eine Zahl, welche zur Darstellung der Zahl $m + n\varrho$ in der Form $a_1 + b_1\sigma_1$ sich eignet, so läßt sich $a + b\sigma$ in der Form $a_1 + b_1\sigma_1$ darstellen.

Durch die Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta,$$

wo $N(a + b\theta) \geqq N(\alpha + \beta\theta) > N(\mu + \nu\theta)$ und $\theta = \varrho$ oder $= \sigma$ ist, ist die Anwendbarkeit des Euklidischen Algorithmus bedingt. Unsere Aufgabe ist diese Gleichung zu bilden.

Der Quotient $\frac{a + b\theta}{\alpha + \beta\theta}$ läßt sich auf die Form $u + v\theta$ bringen, in der u und v rationale Zahlen sind; ist $\theta = \varrho$, so ist $u = \frac{a\alpha + Db\beta}{\alpha^2 + D\beta^2}$, $v = \frac{\alpha b - a\beta}{\alpha^2 + D\beta^2}$, ist $\theta = \sigma = \frac{x + y\varrho}{2}$, so ist $u = \frac{4a(\alpha + \beta x) + \beta b(x^2 + Dy^2)}{\beta^2(x^2 + Dy^2) + 4\alpha(\alpha + \beta x)}$ und

$$v = \frac{4(\alpha b - a\beta)}{\beta^2(x^2 + Dy^2) + 4\alpha(\alpha + \beta x)}.$$

Setzen wir $u = p + \xi$, $v = q + \eta$, wo p und q ganze Zahlen sind, so ist

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + (\alpha + \beta\theta)(\xi + \eta\theta).$$

Das Produkt $(\alpha + \beta\theta)(\xi + \eta\theta) = \mu + \nu\theta$ ist ganz.

Ist $N(\xi + \eta\theta) = 0$, so ist $G(a + b\theta, \alpha + \beta\theta) = \alpha + \beta\theta$, dazu muß $\xi = 0$, $\eta = 0$ sein.

Die $N(\mu + \nu\theta)$ ist der $N(\xi + \eta\theta)$ proportional.

Damit der Euklidische Algorithmus anwendbar wird, muß

$$N(\xi + \eta\theta) < 1$$

sein. Diese Bedingung ist nicht nur notwendig, sondern auch hinreichend.

Es kommt zuvörderst darauf an, die $N(\xi + \eta\theta)$ möglichst zu verkleinern.

Die Verkleinerung von $N(\xi + \eta\theta)$ ist von der Wahl der Zahl σ unabhängig.

Wir werden $\sigma = \vartheta = \frac{1 + \varrho}{2}$ setzen.

Es ist $\vartheta^2 = \vartheta - \frac{1 + D}{4}$ und $N(a + b\vartheta) = a^2 + b^2\frac{1 + D}{4} + ab$.

Die Form $a + b\vartheta$ werden wir benutzen nur wenn $\frac{1 + D}{4}$ ganz ist.

Die Zahl $a + b\vartheta$ ist bei ganzzahligen a und b eine ganze Zahl.

Es ist $\frac{a + b\vartheta}{\alpha + \beta\vartheta} = \frac{4a(\alpha + \beta) + \beta b(1 + D)}{\beta^2(1 + D) + 4\alpha(\alpha - \beta)} + \frac{4(\alpha b - a\beta)}{\beta^2(1 + D) + 4\alpha(\alpha + \beta)}\vartheta$.

Ist $D = 4t + 1$ so ist $\theta = \varrho$ und $N(\xi + \eta\theta) = \xi^2 + D\eta^2$. Den möglichst kleinsten Wert bekommt dieser Ausdruck, wenn $|\xi| \leqq \frac{1}{2}$ und $|\eta| \leqq \frac{1}{2}$.

Die Bedingung $N(\xi + \eta\varrho) < 1$ ist für $D = 1$ und $= 2$ immer erreichbar.

Ist $D = 4t + 3$, so ist $\theta = \vartheta$, $N(\xi \pm \eta\theta) = \xi^2 + \eta^2 \cdot \frac{1+D}{4} \pm \xi\eta$ und damit $N(\xi + \eta\vartheta) < 1$, muß $|\eta| < \frac{2}{\sqrt{D}}$ und $\left|\xi + \frac{\eta}{2}\right| < 1$.

Damit $N(\xi + \eta\vartheta)$ den möglichst kleinsten Wert annimmt, setzen wir $|\eta| < \frac{1}{2}$ und $|\xi| < \frac{1}{2}$ wenn $|\eta| > |1 - 2\xi|$ wird oder $|\eta| < \frac{1}{2}$ und $\frac{1}{2} < |\xi| < 1$ im entgegengesetzten Fall.

Für $D = 3$ oder 7 und 11 ist der Euklidische Algorithmus immer anwendbar.

Ist die Ungleichung $N(\xi + \eta\theta) < 1$ erreichbar, so kommen wir durch Verkleinerung der $N(\mu + \nu\theta)$ entweder zu $N(\mu + \nu\theta) = 1$ oder $= 0$. Im ersten Fall haben $a + b\theta$ und $\alpha + \beta\theta$ keine gemeinschaftlichen Faktoren außer den Einheiten, im zweiten finden wir einen gr. gem. Teiler.

Ist $N(\xi + \eta\theta) \geqq 1$, so wird in der Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$
$$N(\mu + \nu\varrho) > N(\alpha + \beta\theta)$$

und der Euklidische Algorithmus ist nicht anwendbar, es kann aber der Fall sein, daß

$$N(\mu + \nu\theta) < N(a + b\theta)$$

und wir kommen in diesem Fall auf die Frage, ob sich die Aufgabe $G(a + b\theta, \alpha + \beta\theta)$ zu finden auf die Auffindung von $G(\mu + \nu\theta, \alpha + \beta\theta)$, wo die Norm der einen Zahl verkleinert ist, reduzieren läßt. Diese Frage muß mit nein beantwortet werden.

Es ist nun noch die Frage zu beantworten, ob wir nicht auch in dem Fall

$$N(\mu + \nu\theta) > N(\alpha + \beta\theta)$$

durch weitere Division zum Ziel kommen. Diese Frage muß auch mit nein beantwortet werden.

Wir haben den Euklidischen Algorithmus anzuwenden versucht durch die Bildung der Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$

und dazu haben wir $a + b\theta$ durch $\alpha + \beta\theta$ dividiert. Ist

$$N(\mu + \nu\theta) > N(\alpha + \beta\theta),$$

so ist noch die Frage zu erledigen, ob sich der Euklidische Algorithmus nicht durch Division von $\alpha + \beta\theta$ durch $a + b\theta$ anwenden läßt. Diese Frage muß auch mit nein beantwortet werden.

Aus diesen Überlegungen folgt:

Der Euklidische Algorithmus kann nicht für die quadratischen imaginären Zahlen in irgend einem Sinn verändert werden.

Von einer allgemeinen Anwendung des Euklidischen Algorithmus kann mit Ausnahme von $R(\sqrt{-1})$, $R(\sqrt{-2})$, $R(\sqrt{-3})$, $R(\sqrt{-7})$, $R(\sqrt{-11})$ für keinen einzelnen von den zu untersuchenden Körpern die Rede sein.

Der Satz: „Ist der Euklidische Algorithmus anwendbar, so ist die Zerlegung in unzerlegbare Faktoren eindeutig," ist nicht umkehrbar.

Es ist von Interesse sagen zu können, ob der Euklidische Algorithmus versagt oder angewandt werden kann bevor die Division ausgeführt worden ist. Ein solches allgemeines Kriterium ist unmöglich.

Der Euklidische Algorithmus versagt wenn $p = q = 0$ ist.

Wenn etwa in $\alpha + \beta\theta$ die Zahlen α und β eine gewisse Relation erfüllen, so versagt der Euklidische Algorithmus, auf $a + b\theta$ und $\alpha + \beta\theta$ angewandt, bei allen noch möglichen Zahlen $a + b\theta$ und umgekehrt.

Der Fall $p = 0$, $q = 0$, also ein Fall, wo der Euklidische Algorithmus versagt, läßt sich durch das folgende Kriterium angeben.

Ist $\theta = \varrho$, so ist es

$$4N(a + b\varrho) \leqq (1 + D)N(\alpha + \beta\varrho)$$

Ist $\theta = \vartheta$, so ist es:

$$16N(a + b\vartheta) \leqq (25 + D)N(\alpha + \beta\theta).$$

Daneben besteht noch die Bedingung

$$N(a + b\theta) \geqq N(\alpha + \beta\theta).$$

Wenn die Ungleichung

$$N(\xi + \eta\theta) < 1$$

in der angegebenen Weise nicht erfüllt werden kann, so ist die Gleichung

$$a + b\theta = (\alpha + \beta\theta)(p + q\theta) + \mu + \nu\theta$$

überhaupt nicht erfüllbar, und der Euklidische Algorithmus versagt vollständig.

Beispiel I. Es soll $G(8 + 3\sqrt{-3}, -1 + 4\sqrt{-3})$ gefunden werden

$$G(8 + 3\sqrt{-3}, -1 + 4\sqrt{-3}) = 2 - \sqrt{-3}.$$

Beispiel II. Es ist $G\left(\frac{13 + \sqrt{-19}}{2}, \frac{5 + \sqrt{-19}}{2}\right)$ zu bestimmen.

Hier versagt der Euklidische Algorithmus.

In derartigen Fällen müssen wir uns demnach nach einem dem Prinzipe nach von dem Euklidischen verschiedenen Algorithmus umsehen.

Die Aufsuchung des größten gemeinschaftlichen Teilers von $a + b\theta$ und $\alpha + \beta\theta$ durch Zerlegung dieser Zahlen in unzerlegbare Faktoren kann nicht dieser gesuchte Algorithmus sein.

§ 4. Die Bestimmung des größten gem. Teilers für eindeutig zerlegbare quadratische imaginäre Zahlen mittels der Normen dieser Zahlen.

In diesem § ist das folgende Verfahren begründet.

Wir bestimmen

$$G(m^2+Dn^2,\ r^2+Ds^2)=k,$$

es seien

$$k,\ k_1,\ k_2,\ \ldots\ k_{h-1},\ 1$$

alle Teiler von k.

Wir bestimmen alle ganzzahligen Lösungspaare der Gleichung

$$x^2+Dy^2=4k.$$

Sie seien

$$x_{01},\ y_{01};\ x_{02},\ y_{02},\ \ldots,\ x_{0l},\ y_{0l};$$

wir dividieren $m+n\varrho$ durch alle wesentlich verschiedenen Zahlen der Reihe

$$z_{01}\pm w_{01}\varrho,\ \ldots,\ z_{0l}\pm w_{0l}\varrho,$$

wo $z_{01}=\frac{x_{01}}{2}$, $w_{01}=\frac{y_{01}}{2}$, ... bis wir zu einem ganzen Quotienten $\frac{m+n\varrho}{z_{0g}+w_{0g}\varrho}$ oder $\frac{m+n\varrho}{z_{0g}-w_{0g}\varrho}$ kommen. Ist dann auch $\frac{r+s\varrho}{z_{0g}+w_{0g}\varrho}$ bzw. $\frac{r+s\varrho}{z_{0g}-w_{0g}\varrho}$ ganz, so ist $G(m+n\varrho,\ r+s\varrho)=z_{0g}+w_{0g}\varrho$ oder $z_{0g}-w_{0g}\varrho$.

Ist das mit keiner Zahl $z_{0g}\pm w_{0g}\varrho$ erreicht, dann lösen wir die Gleichung

$$x^2+Dy^2=4k_1$$

auf. Die Lösungspaare heißen

$$x_{11},\ y_{11};\ x_{12},\ y_{12};\ \ldots\ x_{1e},\ y_{1e}.$$

Wir verfahren mit den Zahlen $z_{11}\pm w_{11}\varrho,\ \ldots\ z_{1e}\pm w_{1e}\varrho$ genau so wie mit den Zahlen $z_{01}\pm w_{01}\varrho,\ \ldots,\ z_{0l}\pm w_{0l}\varrho$ bis wir entweder zu einer Gleichung

$$x^2+Dy^2=k_h$$

kommen, bei der $m+n\varrho$ und $r+s\varrho$ durch eine Zahl $z_{hg}+w_{hg}\varrho$ oder $z_{hg}-w_{hg}\varrho$ dividiert, ganze Quotienten ergeben, dann ist diese Zahl $=G(m+n\varrho,\ r+s\varrho)$, oder bis wir zur Gleichung

$$x^2+Dy^2=4$$

kommen und dann ist $m+n\varrho$ mit $r+s\varrho$ teilerfremd.

Dieses Verfahren ist immer anwendbar. Der größte gem. Teiler wird durch eine endliche Anzahl von Proben gefunden.

Der Euklidische Algorithmus, so lange er anwendbar ist, führt auch zum Ziel nur durch Probieren und mittels einer endlichen Probeanzahl.

In dieser Weise kann man den größten gem. Teiler auch für eine beliebige Anzahl gegebener Zahlen bestimmen.

Beispiel I. Es ist $G\left(18 + 23\varrho, \frac{45 - 79\varrho}{2}\right)$ zu suchen $\varrho = \sqrt{-3}$.

In diesem Beispiel haben wir jedes Mal sechs nicht wesentlich verschiedene Zahlen zu unterscheiden

$$G\left(18 + 23\varrho, \frac{45 - 79\varrho}{2}\right) = 4 - 5\varrho.$$

Beispiel II. Es ist $G\left(\frac{283 - 151\varrho}{2}, \frac{91 - 15\varrho}{2}\right)$ zu bestimmen $\varrho = \sqrt{-7}$

$$G\left(\frac{283 - 151\varrho}{2}, \frac{91 - 15\varrho}{2}\right) = \frac{3 + \sqrt{-7}}{2}.$$

§ 5. Die Zerlegung von eindeutig zerlegbaren quadratischen imaginären Zahlen in unzerlegbare Faktoren.

Die quadratische Gleichung $x^2 + Dy^2 = 4k_h$ ergibt auch die Zerlegung von $m + n\varrho$ in unzerlegbare Faktoren.

Es sind in diesem § die folgenden Sätze bewiesen:

Ist $m + n\varrho$ eine unzerlegbare Zahl, so ist es $m - n\varrho$ auch. Hat eine rationale Primzahl p einen Faktor r, so ist $r = \pm p$, hat sie einen Faktor $s\varrho$, so ist $s\varrho = \pm \varrho$ und das ist nur möglich, wenn $p = D$ ist.

Die Zahl ϱ ist in jedem ihr entsprechenden Körper eine unzerlegbare Zahl.

Hat die Zahl p einen unzerlegbaren Teiler $r + s\varrho$, wo r und s von 0 verschieden sind, so ist

$$r^2 + Ds^2 = p.$$

Erfüllen umgekehrt r und s die Gleichung $r^2 + Ds^2 = p$ und sind $r = \alpha$ oder $\frac{\alpha}{2}$ und $s = \beta$ oder $\frac{\beta}{2}$, wo α und β ganz sind, so ist $r + s\varrho$ eine unzerlegbare Zahl.

Wenn p in Faktoren zerlegbar ist, so sind das 2 konjugierte unzerlegbare Zahlen, oder p ist ein Quadrat einer unzerlegbaren Zahl.

Wenn $x^2 + Dy^2 = p$ ein Lösungspaar α, β hat, so kann $x^2 + Dy^2 = 4p$ nur das Lösungspaar 2α, 2β haben.

Wenn $x^2 + Dy^2 = p$ ein Lösungspaar hat, so ist dies das einzige (Eulersches Kriterium).

Ist p Nichtrest der Zahl D, so ist p in $R(\sqrt{-D})$ eine unzerlegbare Zahl, die Gleichung $x^2 + Dy^2 = 4p$ sagt aber mehr aus. Die Feststellung, ob p quadratischer Rest von D ist oder nicht, ist nicht einfacher wie die Auflösung dieser Gleichung, wodurch nicht nur die Zerlegbarkeit bewiesen, sondern auch die Zerlegung selbst angegeben wird.

Das Verfahren selbst unterscheidet sich von dem im vorigen § angegebenen dadurch, daß wir die Reihe

$$1, l_1, l_2, \ldots l_n,$$

wo $1, l_1, \ldots l_n$ alle Faktoren von $N(m + n\varrho) = l_n$ sind, nach steigender Größe ordnen und die kleinste Zahl l_h, der ein passendes Lösungspaar der Gleichung $x^2 + Dy^2 = 4l_h$ entspricht, bietet einen unzerlegbaren Teiler der Zahl $m + n\varrho$.

Beispiel. Es soll die Zahl $\frac{429 + 129\sqrt{-11}}{2}$ in unzerlegbare Faktoren zerlegt werden

$$\frac{429 + 129\sqrt{-11}}{2} = \frac{1 + \sqrt{-11}}{2} \cdot \left(\frac{1 - \sqrt{-11}}{2}\right)^3 \cdot \sqrt{-11} \cdot (2 - 3\sqrt{-11}).$$

Die Lösungspaare der Gleichung $x^2 + Dy^2 = 4k$ oder $= 4l$ lassen sich für kleinzahlige k oder l leicht bestimmen mittels einer Tabelle der Quadratzahlen, infolgedessen ist auch eine Tabelle der Quadratzahlen von 1 bis 100 angegeben.

§ 6. Behandlung der Gleichung $x^2 + Dy^2 = k$ für große k.

Dieser § enthält die Auflösung der quadratischen Gleichung

$$x^2 + Dy^2 = k,$$

welche bei der angegebenen Normmethode eine Hauptrolle spielt. Die ist nach Gauß „Disqu. arithmeticae“ § 323 durchgeführt, es sind aber dabei die Vereinfachungen, welche der Koeffizient 1 bei x^2 mit sich bringt, ausgenutzt. Diese ist durch die Ausrechnung eines Beispiels

$$x^2 + 43y^2 = 3517669$$

erläutert. Das Ziel dieses § ist, die Schwierigkeiten, welche entstehen, wenn k groß ist, möglichst zu beseitigen.

§ 7. Die Faktorenzerlegung der quadratischen Form $a^2 + Db^2$.

Auch die Zerlegung in rat. Faktoren der rat. Zahl $N(m + n\varrho)$ bietet große Schwierigkeiten. Nach der Ausschaltung der Faktoren 2^r, $G(a, b)$, und D bleiben nur noch ungerade Teiler der quadratischen Form $a^2 + Db^2$ zu bestimmen. Für diese ist eine Tabelle angegeben, wo sie in linearer Form dargestellt sind. Die Bildung dieser Tabelle beruht auf folgendem.

Hat die Kongruenz $x^2 + Dy^2 \equiv 0 \pmod{p}$ ein Lösungspaar x, y, wo x, y relativ prim sind, so hat auch die Kongruenz $u^2 + D \equiv 0 \pmod{p}$ eine Lösung und umgekehrt.

Alle ungeraden Teiler der Zahl $a^2 + 2b^2$ sind in der Eorm $8t + 1$ und $8t + 3$ enthalten.

Ist D eine Primzahl der Form $4n + 3$ und p ein ungerader Teiler der Zahl $a^2 + Db^2$, so ist

$$\left(\frac{p}{D}\right) = 1.$$

Ist D eine Primzahl der Form $4n+1$ und p ein Teiler von a^2+Db^2, so ist $\left(\frac{p}{D}\right) = (-1)^{\frac{p-1}{2}}$ d. h. $\left(\frac{p}{D}\right) = 1$, wenn $p = 4m + 1$ und $\left(\frac{p}{D}\right) = -1$, wenn $p = 4m + 3$ ist.

Beispiel. Es sollen alle Faktoren von $378^2 + 19 \cdot 43^2 = 178015$ bestimmt werden

$$178015 = 5 \cdot 35603.$$

Die Zahl 35603 ist eine Primzahl. Das kann man durch Ausprobieren mit $[\sqrt{35603}] = 188$ Zahlen feststellen. Wenn wir aber die Formen der linearen Teiler benutzen, so brauchen wir dazu nur $\left[\frac{188}{38}\right] \cdot 9 = 4 \cdot 9 = 36$ Zahlen auszuprobieren. Haben wir die Möglichkeit, nur Primzahlen in dem Intervall von 1 bis 188 zu probieren, so sind das 42 Zahlen. Mit Benutzung obiger Formen bleiben aber nur 17.

Lebenslauf.

Ich, Jacob Schatunovsky, bin am 9. Oktober 1876 in Bogutschar am Don in Rußland geboren. Meine ersten Lebensjahre verbrachte ich in Wosnesensk (Gouvernement Cherson) und absolvierte die dortige städtische Schule. Einige Jahre nachher ging ich nach Odessa. Dort gab ich Stunden und bereitete mich zum Abiturientenexamen vor, das ich im Jahre 1901 in Kutais (Kaukasus) bestand. Im selben Jahr war ich in der Universität Odessa immatrikuliert. Die Zeit von 1901 bis 1906 ließ nur perioden-weise das Studium zu. Im Jahre 1906 kam ich dann nach Deutschland, um speziell Mathematik zu studieren. Hiermit verbrachte ich drei Semester in Berlin. Von 1907 bis 1911 studierte ich in Straßburg.

Meinen hoch verehrten Lehrern und Freunden Herren Prof. B. Kagan, Prof. S. Schatunovsky, Prof. E. Bunitzky an der Universität Odessa, sowie meinem hoch verehrten Lehrer Geheimrat Prof. Dr. H. A. Schwarz an der Universität Berlin, Prof. Dr. H. Weber, Prof. Dr. I. Wellstein, Prof. Dr. T. Reye und Prof. Dr. F. Schur an der Universität Straßburg fühle ich mich in dauernder Dankbarkeit verpflichtet.